(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－507295
(P2002－507295A)
(43)公表日　平成14年３月５日(2002.3.5)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｚ
Ｈ０４Ｌ　12/24		Ｈ０４Ｌ	11/08	
12/28			11/20	Ｂ
12/66				

審査請求 未請求　予備審査請求 有　（全 66 頁）

(21)出願番号　特願平11－500378
(86)(22)出願日　平成10年５月28日(1998.5.28)
(85)翻訳文提出日　平成11年11月29日(1999.11.29)
(86)国際出願番号　ＰＣＴ／ＵＳ９８／１０８１７
(87)国際公開番号　ＷＯ９８／５４６４４
(87)国際公開日　平成10年12月３日(1998.12.3)
(31)優先権主張番号　０８／８６５，４８２
(32)優先日　平成９年５月29日(1997.5.29)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＡ，ＧＢ，ＪＰ

(71)出願人　３コム　コーポレイション
アメリカ合衆国　カリフォルニア州　95052－8145　サンタ　クララ　ベイフロント　プラザ　5400　ピーオーボックス　58145　メイル　ストップ　1308
(72)発明者　ネセット　ダニー　エム
アメリカ合衆国　カリフォルニア州　94555　フリーモント　ワパッシュ　リヴァー　プレイス　34810
(72)発明者　シェラー　ウィリアム　ポール
アメリカ合衆国　カリフォルニア州　94506　ダンヴィル　ペッパーウッド　ドライヴ　850
(74)代理人　弁理士　中村　稔　（外９名）

(54)【発明の名称】　多層型ファイアウオールシステム

(57)【要約】
多数のプロトコル層で働くセキュリティ機能を有するノードを含むネットワーク(10)にセキュリティを確立するシステムが提供される。リモートアクセス装置(13)、ルータ(14)、スイッチ(12)、中継器(16)、及びセキュリティ機能を有するネットワークカード(15)のような多数のネットワーク装置は、ネットワークに分散されたファイアウオール機能の実施に貢献するように構成される。種々のネットワーク装置においてネットワークの多数の層全体にわたりファイアウオール機能を分散することにより、浸透したファイアウオールが実施される。浸透した多層ファイアウオールは、ファイアウオールがいかに振舞うべきかを定義するポリシーデータを受け入れるポリシー定義要素(11)を備えている。又、多層ファイアウオールは、定義されたポリシーを実施するのに使用されるネットワークデバイスの集合を含む。ネットワークデバイスのこの集合において多数のプロトコル層にわたって動作するセキュリティ機能は、ポリシー定義要素により整合され、特定のデバイスがネットワークの当該部分に関与するポリシーの部分を実施するようにする。

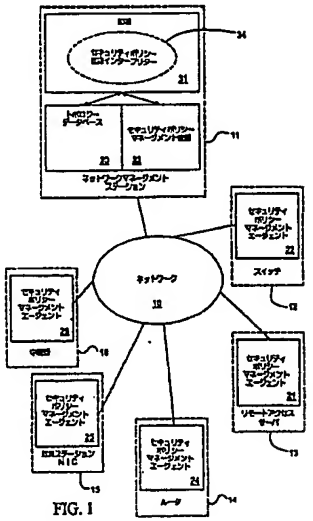

FIG. 1

【特許請求の範囲】

１．複数の形式のノードを含むネットワークにセキュリティを与えるシステムであって、ネットワーク内のノードセットのノードは、対応するノード形式に適応したコンフィギュレーションデータに応答して実行されるセキュリティ機能を含むようなシステムにおいて、

ネットワーク内のノードセットにおいて働くセキュリティ機能と、ノードセット内のノードの相互接続とに関する情報を記憶するトポロジーデータ記憶装置と

上記トポロジーデータ記憶装置に接続され、ネットワーク内のノード間で実施されるべきセキュリティポリシーを指示するセキュリティポリシーステートメントを受け取る入力を含むコンフィギュレーションインターフェイスと、

上記ネットワーク；コンフィギュレーションインターフェイス及びトポロジーデータ記憶装置に接続され、セキュリティポリシーステートメントを、ネットワーク内の複数の形式のノードに対するコンフィギュレーションデータに変換し、そしてそのコンフィギュレーションデータをノードへと搬送するリソースを含むコンフィギュレーションドライバーと、

を備えたことを特徴とするシステム。

２．上記ノードセットは、フィルタパラメータに基づいて媒体アクセス制御ＭＡＣ層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ＭＡＣ層フィルタリングのためのフィルタパラメータを含む請求項１に記載のシステム。

３．上記ノードセットは、フィルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ネットワーク層フィルタリングのためのフィルタパラメータを含む請求項１に記載のシステム。

４．上記ノードセットは、フィルタパラメータに基づいて搬送層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、搬送層フィルタリングのためのフィルタパラメータを含む請求項１に記載のシステム。

５．上記ノードセットは、フィルタパラメータに基づきアプリケーション層フ

ィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、

アプリケーション層フィルタリングのためのフィルタパラメータを含む請求項１に記載のシステム。

６．上記セキュリティ機能は、認証プロトコルを含む請求項１に記載のシステム。

７．上記セキュリティ機能は、オーデットを含む請求項１に記載のシステム。

８．上記セキュリティ機能は、許可を含む請求項１に記載のシステム。

９．上記ノードセットは、中継器の機能を実行するノードを含み、そして上記セキュリティ機能は、中継器の機能に媒体アクセス制御ＭＡＣ層フィルタリングを含む請求項１に記載のシステム。

１０．上記ノードセットは、データリンク層スイッチの機能を実行するノードを含み、そして上記セキュリティ機能は、スイッチ機能に媒体アクセス制御ＭＡＣ層フィルタリングを含む請求項１に記載のシステム。

１１．上記ノードセットは、ネットワーク層ルート指定機能を実行するノードを含み、そして上記セキュリティ機能は、ルート指定機能にネットワーク層フィルタリングを含む請求項１に記載のシステム。

１２．上記ノードセットは、多数のプロトコル層ルート指定機能を実行するノードを含み、そして上記セキュリティ機能は、認証機構を含む請求項１に記載のシステム。

１３．上記ノードセットは、ネットワーク層ルート指定機能を実行するノード及びデータリンク層スイッチ機能を実行するノードを含み、そして上記セキュリティ機能は、媒体アクセス制御ＭＡＣ層フィルタリング及びネットワーク層フィルタリングを含む請求項１に記載のシステム。

１４．上記ノードセットは、多数のプロトコル層ルート指定機能を実行するノードを含み、そして上記セキュリティ機能は、認証を含む請求項１３に記載のシステム。

１５．上記トポロジーデータ記憶装置は、ノードセットの外部のノードへ至るネットワークリンクに接続されたノードを指示するデータを含む請求項１に記載

のシステム。

１６．上記トポロジーデータ記憶装置は、ノードセットの外部のノードへ至るネットワークリンクに接続されたノードと、セキュリティポリシーを実施できる能動的ノードと、セキュリティポリシーを実施できないか又は実施する信頼性のない受動的ノードとを指示するデータを含み、そして

上記セキュリティポリシーステートメントは、能動的ノードと、受動的ノードと、ノードセットの外部のノードへ至るネットワークリンクに進行する通信とに対してセキュリティポリシーを指示する請求項１に記載のシステム。

１７．上記コンフィギュレーションインターフェイスは、スクリプト言語を解読してセキュリティポリシーステートメントを決定するスクリプトインタープリターを含む請求項１に記載のシステム。

１８．上記トポロジーデータ記憶装置は、セキュリティポリシーを実施できる能動的ノードと、セキュリティポリシーを実施できないか又は実施する信頼性のない受動的ノードとを指示するデータを含む請求項１に記載のシステム。

１９．上記セキュリティポリシーステートメントは、１つ以上の最終ステーションのソースセットと、１つ以上の最終ステーションの行先セットとの間の通信に対するセキュリティポリシーを指示する請求項１８に記載のシステム。

２０．上記コンフィギュレーションドライバは、受動的ノードにリンクされた能動的ノードに対してコンフィギュレーションデータを発生することにより受動的ノードのセキュリティポリシーを実施するリソースを含む請求項１８に記載のシステム。

２１．上記スクリプト言語は、ソースセット識別子、行先セット識別子、通信アクティビティ識別子、及び識別されたソースセットと識別された行先セットとの間の識別された通信アクティビティに対するルールを含むセキュリティポリシーステートメントを指定するシンタックスを含む請求項１７に記載のシステム。

２２．上記シンタックスは、更に、ルールを実施すべき位置の識別子を含む請求項２１に記載のシステム。

２３．上記コンフィギュレーションドライバーは、トポロジーデータ記憶装置

のデータに基づいて実施できないセキュリティポリシーステートメントを識別するためのリソースを含む請求項２１に記載のシステム。

２４．ノードセットの特定ノードと通信する永続的記憶能力を有するコンフィギュレーション記憶装置を備え、そして上記コンフイギュレーションドライバーは、特定ノードに対するコンフィギュレーションデータをコンフィギュレーション記憶装置に送信する請求項１に記載のシステム。

２５．上記コンフィギュレーション記憶装置は、通信リンクによって特定ノードに接続される請求項２４に記載のシステム。

２６．上記トポロジーデータ記憶装置は、ネットワーク層アドレス、媒体アクセス制御ＭＡＣ層アドレス、ユーザ識別子、特定ノードがセキュリティポリシーを実施する信頼があるかどうか、実施できるセキュリティポリシーの形式、及び他のノードへのその接続を含む特定ノードの情報を与えるデータ構造体を備えている請求項１に記載のシステム。

２７．上記セキュリティポリシーステートメントは、ネットワークの１つ以上の最終ステーションを含むソースセットと、ネットワークの１つ以上の最終ステーションを含む行先セットとの間の通信に対するセキュリティポリシーを指示し、そして上記コンフィギュレーションドライバーは、ネットワークのノードセット内の指示されたセキュリティポリシーを実施することのできるカット頂点セットのノードを識別しそしてカット頂点セットのノードにコンフィギュレーションデータを確立するためのリソースを含む請求項１に記載のシステム。

２８．上記カット頂点セットは、最小のカット頂点セットより成る請求項２７に記載のシステム。

２９．複数の形式のノードを含むネットワークにセキュリティを与えるシステムであって、ネットワーク内のノードセットのノードは、対応するノード形式に適応したコンフィギュレーションデータに応答して実行されるセキュリティ機能を含むようなシステムにおいて、

ネットワーク内のノードセットのセキュリティ機能と、ノードセット内のノードの相互接続とに関する情報を記憶するトポロジーデータ記憶装置であって、１

つ以上のプロトコル層におけるアドレス、特定ノードがセキュリティポリシーを実施する信頼性があるかどうか、特定ノードが実施できるセキュリティポリシーの形式、及び特定ノードと他のノードとの接続を含む特定ノードの情報を与えるデータ構造体を有するトポロジーデータ記憶装置と、

上記トポロジーデータ記憶装置に接続されたコンフィギュレーションインターフェイスであって、このインターフェイスは、ネットワークにおける１つ以上の終端ステーションのソースセットと１つ以上の終端ステーションの行先セットとの間で実施されるべきセキュリティポリシーを指示するセキュリティポリシーステートメントを受け取る入力と、スクリプト言語を解読してセキュリティポリシーステートメントを決定するためのスクリプトインタープリターとを含み、上記スクリプト言語は、ソースセット識別子、行先セット識別子、通信アクティビティ識別子、及び識別されたソースセットと識別された行先セットとの間の識別された通信アクティビティに対するルールを含むセキュリティポリシーステートメントを指定するシンタックスを含むようなコンフィギュレーションインターフェイスと、

上記ネットワーク、コンフィギュレーションインターフェイス及びトポロジーデータ記憶装置に接続され、セキュリティポリシーステートメントを、ネットワーク内の種々の形式のノードに対するコンフィギュレーションデータに変換し、そしてそのコンフィギュレーションデータをノードへと搬送するリソースを含むコンフィギュレーションドライバーと、

を備えたことを特徴とするシステム。

３０．上記ノードセットは、フィルタパラメータに基づいて媒体アクセス制御ＭＡＣ層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ＭＡＣ層フィルタリングのためのフィルタパラメータを含む請求項２９に記載のシステム。

３１．上記ノードセットは、フィルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ネットワーク層フィルタリングのためのフィルタパラメータを含む請求項２９に

記載のシステム。

３２．上記ノードセットは、フィルタリングパラメータに基づいて搬送層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、搬送層フィルタリングのためのフィルタパラメータを含む請求項２９に記載のシステム。

３３．上記ノードセットは、フィルタパラメータに基づきアプリケーション層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、アプリケーション層フィルタリングのためのフィルタパラメータを含む請求項２９に記載のシステム。

３４．上記トポロジーデータ記憶装置は、セキュリティポリシーを実施できる能動的ノードと、セキュリティポリシーを実施できないか又は実施する信頼性のない受動的ノードとを指示するデータを含む請求項２９に記載のシステム。

３５．上記トポロジーデータ記憶装置は、ノードセットの外部のノードへ至るネットワークリンクに接続されたノードを指示するデータを含む請求項２９に記載のシステム。

３６．上記セキュリティポリシーステートメントは、ノードセットの外部のノードへ至るネットワークリンクに進行する通信に対するセキュリティポリシーを指示する請求項３５に記載のシステム。

３７．上記シンタックスは、更に、ルールを実施すべき位置の識別子を含む請求項２９に記載のシステム。

３８．上記コンフィギュレーションドライバーは、トポロジーデータ記憶装置のデータに基づいて実施できないセキュリティポリシーステートメントを識別するためのリソースを備えている請求項２９に記載のシステム。

３９．ノードセットの特定ノードと通信する永続的記憶能力を有するコンフィギュレーション記憶装置を備え、そして上記コンフィギュレーションドライバーは、特定ノードに対するコンフィギュレーションデータをコンフィギュレーション記憶装置に送信する請求項２９に記載のシステム。

４０．上記コンフィギュレーション記憶装置は、通信リンクにより特定のノードに接続される請求項３９に記載のシステム。

４１．上記コンフィギュレーションドライバーは、指示されたセキュリティポリシーを実施することのできるカット頂点セットのノードを識別しそしてカット頂点セットのノードにコンフィギュレーションデータを確立するためのリソースを含む請求項２９に記載のシステム。

４２．上記カット頂点セットは、最小のカット頂点セットより成る請求項４１に記載のシステム。

４３．複数の形式のノードのセットを含むネットワークにファイアウオールシステムを確立する方法であって、ネットワーク内の上記ノードセットのノードは、対応するノードに適応したコンフィギュレーションデータに応答して実行されるセキュリティ機能を含み、上記方法は、

上記ノードセットのノードにおいて働くセキュリティ機能と、上記ノードセットのノードの相互接続とに関する情報を含むトポロジーデータを与え、

上記ノードセットの最終システム間で実施されるべきセキュリティポリシーを指示するセキュリティポリシーステートメントを与え、

上記トポロジーデータに応答して、セキュリティポリシーステートメントを、ノードセットのノードにおいて働くセキュリティ機能に対するコンフィギュレーションデータへと変換し、そして

ネットワーク内のノードにおいてセキュリティ機能にコンフィギュレーションデータを確立する、

という段階を備えたことを特徴とする方法。

４４．上記トポロジーデータは、１つ以上のプロトコル層のアドレス、特定ノードがセキュリティポリシーを実施する信頼があるかどうか、特定ノードが実施できるセキュリティポリシーの形式、及び特定ノードと他のノードとの接続を含む特定ノードの情報を与えるデータ構造体を備えている請求項４３に記載の方法。

４５．セキュリティポリシーステートメントを与える上記段階は、スクリプト言語を解読して、セキュリティポリシーステートメントを決定することを含み、

上記スクリプト言語は、ソース識別子、行先識別子、通信アクティビティ識別子、及び識別されたソースと識別された行先との間の識別された通信アクティビティに対するルールを含むセキュリティポリシーステートメントを指定するためのシンタックスを含む請求項４３に記載の方法。

４６．上記シンタックスは、更に、ルールを実施すべき位置の識別子を含む請求項４５に記載の方法。

４７．上記確立段階は、ノードと通信する永続的な記憶装置にネットワークのコンフィギュレーションデータを送信することを含む請求項４３に記載の方法。

４８．少なくとも１つのノードに対し、ノードと通信する永続的な記憶装置は、ノードにとってローカルであり、そして少なくとも１つの他のノードに対し、ノードと通信する永続的な記憶装置は、ノードから離れている請求項４７に記載の方法。

４９．少なくとも１つのノードに対し、ノードと通信する永続的な記憶装置は、ノードから離れており、ノードにコンフィギュレーションデータを確立する上記段階は、永続的な記憶装置にコンフィギュレーションデータを送信した後に、コンフィギュレーションデータが変化したことをノードのセキュリティ機能に通知することを含む請求項４７に記載の方法。

５０．上記トポロジーデータは、セキュリティポリシーを実施できる能動的ノードと、セキュリティポリシーを実施できないか又は実施する信頼性のない受動的ノードとを指示するデータを含む請求項４３に記載の方法。

５１．上記トポロジーデータは、ノードセットの外部のノードへ至るネットワークリンクに接続されたノードを指示するデータを含む請求項５０に記載の方法。

５２．上記セキュリティポリシーステートメントは、ノードセットの外部のノードへ至るネットワークリンクに進行する通信に対してセキュリティポリシーを指示する請求項５１に記載の方法。

５３．上記変換段階は、受動的ノードのセキュリティポリシーを実施するために、受動的ノードにリンクされた能動的ノードのコンフィギュレーションデータを発生することを含む請求項５０に記載の方法。

５４．上記変換段階は、トポロジーデータ記憶装置のデータに基づいて実施できないセキュリティポリシーステートメントを識別することを含む請求項４３に記載の方法。

５５．上記ノードセットは、フィルタパラメータに基づいてＭＡＣ層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ＭＡＣ層フィルタリングのためのフィルタパラメータを含む請求項４３に記載の方法。

５６．上記ノードセットは、フィルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ネットワーク層フィルタリングのためのフィルタパラメータを含む請求項４３に記載の方法。

５７．上記ノードセットは、フィルタパラメータに基づいて搬送層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、搬送層フィルタリングのためのフィルタパラメータを含む請求項４３に記載の方法。

５８．上記ノードセットは、フィルタパラメータに基づきアプリケーション層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、アプリケーション層フィルタリングのためのフィルタパラメータを含む請求項４３に記載の方法。

５９．上記セキュリティ機能は、許可を含む請求項４３に記載の方法。

６０．上記セキュリティ機能は、認証を含む請求項４３に記載の方法。

６１．上記セキュリティ機能は、オーデットを含む請求項４３に記載の方法。

６２．上記ノードセットは、インターネットプロトコルＩＰフィルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ＩＰフィルタパラメータを含む請求項４３に記載の方法。

６３．上記ノードセットは、インターネットプロトコル及び搬送制御プロトコルＴＣＰ／ＩＰフィルタパラメータに基づいてフィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ＴＣＰ／ＩＰフィルタパラメー

タを含む請求項４３に記載の方法。

６４．複数の形式のノードのセットを含むネットワークにファイアウオールシステムを確立する方法であって、ネットワーク内の上記ノードセットのノードは、対応するノードに適応したコンフィギュレーションデータに応答して実行されるセキュリティ機能を含み、上記方法は、

上記ノードセットのノードにおいて働くセキュリティ機能と、上記ノードセットのノードの相互接続とに関する情報を含むトポロジーデータを与え、

上記ノードセットにおける最終ステーションのソースセットと最終ステーションの行先セットとの間で実施されるべきセキュリティポリシーを指示するセキュリティポリシーステートメントを与え、

トポロジーデータ及びセキュリティポリシーステートメントに応答して、セキュリティポリシーステートメントを実施できるノードより成るカット頂点セットのノードを識別し、これは、ネットワークから除去された場合に、ソースセットを行先セットから分離するものであり、

識別されたカット頂点セット及びセキュリティポリシーステートメントに応答して、カット頂点セットのノードにおいて働くセキュリティ機能に対するコンフィギュレーションデータへと変換し、そして

カット頂点セットのノードにおいてセキュリティ機能にコンフィギュレーションデータを確立する、

という段階を備えたことを特徴とする方法。

６５．上記トポロジーデータは、アドレス、特定ノードがセキュリティポリシーを実施する信頼があるかどうか、特定ノードが実施できるセキュリティポリシーの形式、及び特定ノードと他のノードとの接続を含む特定ノードの情報を与えるデータ構造体を備えている請求項６４に記載の方法。

６６．セキュリティポリシーステートメントを与える上記段階は、スクリプト言語を解読して、セキュリティポリシーステートメントを決定することを含み、上記スクリプト言語は、ソース識別子、行先識別子、通信アクティビティ識別子、及び識別されたソースと識別された行先との間の識別された通信アクティビティに対するルールを含むセキュリティポリシーステートメントを指定するためのシンタックスを含む請求項６４に記載の方法。

６７．上記確立段階は、カット頂点セットのノードと通信する永続的な記憶装置にネットワークのコンフィギュレーションデータを送信することを含む請求項６４に記載の方法。

６８．少なくとも１つのノードに対し、ノードと通信する永続的な記憶装置は、ノードにとってローカルであり、そして少なくとも１つの他のノードに対し、ノードと通信する永続的な記憶装置は、ノードから離れている請求項６７に記載の方法。

６９．上記ノードセットは、インターネットプロトコルＩＰフイルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ＩＰフィルタパラメータを含む請求項６４に記載の方法。

７０．上記ノードセットは、インターネットプロトコル及び搬送制御プロトコルＴＣＰ／ＩＰフィルタパラメータに基づいてフィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ＴＣＰ／ＩＰフィルタパラメータを含む請求項６４に記載の方法。

７１．上記カット頂点セットは、最小のカット頂点セットより成る請求項６４に記載の方法。

【発明の詳細な説明】

多層型ファイアウオールシステム

発明の分野

本発明は、ネットワークのセキュリティ機能を確立して実施することに係り、より詳細には、複数のプロトコル層にセキュリティ機能を確立してネットワークに多層型ファイアウオールを確立するシステムに係る。

先行技術の説明

セキュリティは、いわゆるイントラネットを操作する企業内部と、世界的規模のグローバルデータネットワークとの両面で、ネットワークユーザにとって益々重要なものとなってきている。ネットワークのセキュリティを確保する目的で、著しい技術が開発されている。開発されたセキュリティの特徴は、少なくとも、次の製品分類を含む。（1）フィルタリング、（2）アクセス制御、（3）保護通信、（4）セキュリティ支援、及び（5）セキュリティポリシー管理。

フィルタリングは、パケット又はフレームをそれらのヘッダ又はデータ内の値に基づいてドロップし又は変換することを含む。アクセス制御は、ユーザ又はユーザが開始した通信に、特定の計算リソースへのアクセスを与えねばならないかどうか判断することを含む。保護通信は、制御情報又はデータが変更もされないし無許可の個人によって読み取られもしないよう確保するプロセスを指す。セキュリティ支援製品形式は、ネットワークデバイスにおいてシステムの他の部分のセキュリティを確保するための支援を与える。セキュリティポリシー管理は、ネットワークにおいてセキュリティのポリシーを定義するデータを管理することを指す。

このような種類のセキュリティ特徴は、現在のシステムでは、特定のネットワークデバイスにおいて実施される。セキュリティが実施されるネットワークデバイスは、通常のターミナルや最終システムに加えて、次のようなデバイスを含む。（1）ネットワークインターフェイスカード（ＮＩＣ）及びモデム、（2）中継器、（3）スイッチ、（4）ルータ、（5）ラインサーバ、パケットサーバ及びアクセスサーバを含むリモートアクセス装置、及び（6）ネットワークマネージメントシステム。特定の製品ファミリーにセキュリティを確立するための製品

は存

在するが、ネットワークに見られる種々の全ての装置分類において製品の利点を採り入れるシステムは、膨大な管理を必要とする。種々様々なネットワーク中間装置及びターミナルを伴うネットワークにおいては、全ての種々のプロトコルレベル及び全ての種々のシステムにおいてセキュリティポリシーの確立を管理するためのアドミニストレータが必要とされる。

例えば、ある公知システムでは、仮想ローカルエリアネットワーク（ＶＬＡＮ）と称する構成を確立することができる。ＶＬＡＮを構成することにより、グループのメンバーシップが制御される。例えば、ポート番号、媒体アクセス制御アドレス、層３プロトコル形式、層３アドレス、及び層３パケットのパターンに一致するユーザ定義基準を使用して、このような装置におけるＶＬＡＮメンバーシップを定義することができる。同様のパターンマッチングは、例えば、層３ないし７のプロトコルデータを含んでもよい。他のシステムは、リモートアクセスシステムにおいてコールごとのフィルタリングをサポートする。これは、顧客が色々な種類のトラフィックをユーザごとに許可又は拒絶できるようにする。種々様々な他のセキュリティシステムも市場で入手できる。

しかしながら、種々のセキュリティ特徴、種々のデバイス、及びそれらが動作するプロトコルレベルは、セキュリティ特徴の利用者にとって著しい管理の問題を引き起こす。複雑であるために、ネットワークの全ての層及びデバイス形式にわたって整合したセキュリティポリシーを確立することは困難であると共に、これが首尾良く実施されたとしてもこのようなシステムを維持することは特に困難である。

更に、ネットワークの進歩に伴い、特定のセキュリティ機能に参加することのできない遺産的システムとしばしば称される古い装置が残される。それ故、ネットワークに追加されるセキュリティ機能は、ネットワーク全体に首尾良く浸透できないことがある。或いは又、ネットワークにおける遺産的システムの存在が、セキュリティシステムの整合及び実施を更に複雑なものにする。

従来、専用ネットワークを外部からの侵入に対して保護するルータ及びアプリ

ケーションプロキシーゲートウェイのような境界装置としてファイアウオールが実施されている。しかしながら、おそらく、企業の損失の５０％ないし８０％は、

内部の者の侵入、例えば、不満を抱えた又は機会に恵まれた従業員によるものである。従って、会社のイントラネットに関するほとんどのセキュリティ要求は、内部侵入に対する保護である。

更に、現代企業の経営は、その経済性から、会社にとって外注先での作業や他の会社との共同運営が益々必要になっている。現代企業では情報技術が業務の実施に日に日に浸透してきているので、このような外注作業や共同運営は、会社が電子的手段を用いて互いに情報を共用することを必須とする。この情報が、会社の情報財産の他部分を保持するものから分離された装置において入手できることは稀である。従って、外注作業や共同運営には、会社にとってそのイントラネットの一部分へ別の会社がアクセスするのを許可することが必要となる。更に、各々の外注作業や共同運営の構成は、通常、会社の異なる部門や子会社を伴う。これは、少なくとも１つの外部関係者によりアクセスできる会社の情報財産の割合が著しく大きくなることを意味する。

従来の境界ファイアウオールは、２つの事柄、即ち内部の者による脅迫や、広く分散したデータの外部共用によって生じるセキュリティ要件を満足するのにほとんど適していない。境界ファイアウオールは、内部の者による脅迫に対処するのには全く不適である。それらは、外部の侵入者が会社のイントラネットに侵入するのを排除することを意味するが、内部の者がそれを行うのを阻止することはできない。

会社の情報への外部アクセスを受け入れるためには、必要な情報を流せるように境界ファイアウオールに「ホール」を形成しなければならない。極端な場合に、各部門は、会社のファイアウオールを全く簡単にバイパスして、外注先や共同経営の会社、又はその社員へ直接接続することができる。

これらの要件を満足する１つの解決策は、会社のイントラネットを多数の部分に分割し、そしてそれらの間に境界ファイアウオールを配置することである。この解決策は、価値があるが、会社のイントラネットにボトルネックが生じることになる。即ち、内部のファイアウオールが会社内の業務遂行に悪影響を及ぼす。区画化がより細かくなるにつれて、ファイアウオール区画の外部のリソースへのアクセスは、その遂行性が益々悪くなる。

この問題に対する別の解決策は、ファイアウオールの機能をプロトコルハイアラーキーの下位層へと分散することである。従って、例えば、ネットワークインターフェイスカード、中継器及びスイッチが、あるファイアウオールパケットフィルタリング作業を行う場合には、従来パケットフィルタリングを行っていたルータにおいて相当の処理が軽減され、それ故、所与のコストに対して良好な性能を発揮することができる。更に、ファイアウオールの分散化は、規模組成の良好な機会を与える。即ち、ネットワークが成長するにつれて、フィルタリングを実行するのに使用できるリソースも当然成長する。これは、例えば、内部の境界ファイアウオールにおいて生じることのあるチョークポイントの発生を防止する。

通常、公知技術では、パケットフィルタリングのようなファイアウオール機能は、単一のノード、又は同じファイアウオールルールを伴う同様のノードのグループに設けられる。これらのノードは、ネットワークの外部からの侵入に対してネットワークを保護するためにネットワークの境界に展開される傾向にある。しかしながら、この解決策は、ネットワークの拡張につれて充分に規模を広げることができない。更に、ネットワークセキュリティに対して制御の粒度が非常に粗くなる。実施することのできる種々の異なる解決策は、個々のシステムがネットワーク内でいかに相互作用するか理解することが困難である。更に、これらの個々のシステムは、ネットワーク内部の無許可の行為から保護するために適用したときには、通常、著しい性能上の問題を引き起こす。(例えば、「インターネットファイアウオールの構築(Building Internet Firewalls)」、チャプマン氏等著、オーレイリ&アソシエーツ、１９９５年９月；「インターネットファイアウオール及びセキュリティ(Internet Firewall and Security)」、３コム・テクニカルレポート、１９９６年、セメリア著を参照されたい)。

従って、ネットワークシステムの多数の層にわたり整合されたセキュリティポ

リシーを実行することのできるシステムの実施が要望される。

発明の要旨

本発明は、多数のプロトコル層で動作しそしてセキュリティ機能を有するノードを備えたネットワークにおいてセキュリティを与えるシステムを提供する。ルータ、リモートアクセス装置、スイッチ、中継器及びネットワークカードのような多数のネットワークデバイス、並びにセキュリティ機能を有する最終システムプロセスは、ネットワークにおける分散型ファイアウオール機能の実施に貢献するように構成される。ネットワークのファイアウオール機能を種々のネットワークデバイス及び最終システムに分散することにより、浸透したファイアウオールが実施される。浸透した多層型ファイアウオールは、ファイアウオールがいかに振舞わねばならないかを定義するポリシーデータを受け入れるポリシー定義要素を含む。このポリシー定義要素は、集中化された要素であってもよいし、又はネットワークにわたって分散された要素でもよい。又、多層型ファイアウオールは、定義されたポリシーを実施するのに使用されるネットワークデバイスの集合も含む。多数のプロトコル層にわたりネットワークデバイスのこの集合において動作するセキュリティ機能は、特定のデバイスが、ネットワークの当該部分に関与するポリシーの部分を実施するように、ポリシー定義要素により整合される。

例えば、ネットワークのルータは、トラフィックがルータを横切るところのシステム及びネットワークデバイスに関与するポリシーの部分を実施する。スイッチは、トラフィックがスイッチを横切るところのシステム及びネットワークデバイスに関与するポリシーの部分を実施する。中継器は、トラフィックが中継器を横切るところのシステム及びネットワークデバイスに関与するポリシーの部分を実施する。ネットワークインターフェイスカードは、それが接続されたシステム又はデバイスに関与するポリシーの部分を実施する。更に、多層型ファイアウオールにはネットワークの他の部分が含まれ、例えば、最終システムのオペレーティングシステム及びアプリケーションや、ネットワークトラフィックを制御しそしてネットワークトラフィックを監視するリモートアクセス装置のネットワークマネージメントシステムや、他の補助的なシステム、例えば、本発明の浸透した

多層型ファイアウオールが実施されるネットワークデバイスの集合に含まれるネームサーバ及びファイルサーバが含まれる。

本発明は、多数のネットワークデバイス及び最終システムにおいて整合されたアクセス制御、協働保護通信特徴、及び全体的なセキュリティポリシー管理を与える。セキュリティアドミニストレータには、ネットワークのセキュリティ特性を監視できるようにする便利で且つ明確な制御システムが設けられる。更に、本発明は、セキュリティサービスにおける不必要な冗長性を減少できるようにし、遺産的システムサポートのエリアにおいて著しい顧客の要求を満足し、コスト効率を与え、そして複雑さを低減させる。

従って、本発明は、1つの観点によれば、ノードを含むネットワークにセキュリティを与えるシステムを特徴とすることができる。ネットワークのノードセットにおけるノードは、1つ又は多数のプロトコル層で動作するセキュリティ機能を含み、そしてノードの各形式に適応されたフォーマットを有する構成データに応答してこのようなセキュリティ機能を実行する。システムは、ネットワークのノードセットにおいて動作するセキュリティ機能に関する情報及びネットワークにおけるノードの相互接続に関する情報を記憶するトポロジーデータ記憶装置を備えている。このトポロジーデータ記憶装置にはコンフィギュレーションインターフェイスが接続される。このインターフェイスは、ネットワークのノード間で実施されるべきセキュリティポリシーを指示するセキュリティポリシーステートメントを受け取るための入力を含む。ネットワーク、コンフィギュレーションインターフェイス及びトポロジーデータ記憶装置にはコンフィギュレーションドライバーが接続される。このコンフィギュレーションドライバーは、セキュリティポリシーステートメントを、ネットワークのノードに必要なフォーマットのコンフィギュレーションデータへと変換するリソースであって、各ノードに対して使用できる通信チャンネルを用いてコンフィギュレーションデータをノードへ送信するリソースを含む。

本発明の種々の観点によれば、ノードは、媒体アクセス制御MAC層を含む多数のプロトコル層を実行し、そしてノードセットは、フィルタパラメータに基づ

いてMAC層のフィルタリングを与えるノードを含む。コンフィギュレーションデータは、MAC層のフィルタリングに対するフィルタパラメータを含む。別の観点において、多数のプロトコル層は、インターネットプロトコルIP層のようなネットワーク層を含む。この観点によれば、ノードセットは、フィルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含む。コンフィギュレーションデータは、このようなノードにおけるネットワーク層フィルタリングのためのフィルタパラメータを含む。別の観点によれば、多数のプロトコル層は、インターネットプロトコルを介して動作する搬送制御プロトコルTCPのような搬送層機能を含む。この観点によれば、コンフィギュレーションドライバーは、セキュリティポリシーステートメントを、フィルタリングのような搬送層機能、フィルタリングのようなアプリケーション層機能及び／又はプロトコルスタックの上位層における機能に対するコンフィギュレーションデータに変換するリソースを含む。このような上位層機能は、例えば、認証プロトコル、許可プロトコル、オーデットプロトコル及び他のセキュリティ機能を含む。フィルタリンク、アクセス制御、保護通信及びセキュリティ支援特徴を実行する種々のデバイスは、ネットワークインフラストラクチャーにおいて分散され、そして本発明により整合形態で管理される。

本発明の他の観点によれば、コンフィギュレーションインターフェイスは、セキュリティポリシーステートメントを決定するためにスクリプト言語を解読するスクリプトインタープリターを含む。スクリプト言語は、キーボード又はグラフィックユーザインターフェイスによって入力することができる。スクリプト言語のサポートにおいて、トポロジーデータ記憶装置は、セキュリティポリシーを実施することのできるネットワーク内の能動的ノードと、セキュリティポリシーを実施できないか又はそれを実施する信頼のない受動的ノードとを指示するデータを含む。更に、トポロジーデータ記憶装置は、セキュリティフレームワーク内のノードセットの外部のノードへ至るネットワークリンクに接続されたノードを指示するデータも含む。セキュリティポリシーステートメントは、最終システムのセキュリティポリシーを指示する。能動的ノード、受動的ノード、及びセキュリティネットワークの外部のノードへ至るネットワークリンクに接続されたノードは、ポリシーを実行するように構成される。本発明の別の観点によれば、スクリプト言語は、ソースノード又はソースグループのためのソース識別子と、行先ノード又は行先グループのための行先識別子と、通信アクティビティ識別子と、識別されたソースと識別された行先との間の識別された通信アクティビティのためのルールとを含むセキュリティポリシーステートメントを特定するシンタックスを含む。本発明の１つの観点によれば、シンタックスは、更に、ルールを実施すべき位置（即ち、ソース、行先、ソース及び行先の両方、或いは中間ノード）の識別子を含む。

本発明の更に別の観点によれば、セキュリティポリシーステートメントは、ネットワーク内の１つ以上の最終ステーションを含むソースセットと、ネットワーク内の１つ以上の最終ステーションを含む行先セットとの間で通信するためのセキュリティポリシーを指示する。コンフィギュレーションドライバーは、ネットワークのノードセット内の指示されたセキュリティポリシーを実施することのできるノードのカット頂点セットを識別すると共にそのカット頂点セット内のノードにおいてコンフィギュレーションデータを確立するためのリソースを含み、ここで、カット頂点セットは、ネットワークから除去された場合にソースセットを行先セットから分離する能動的ノードより成る。最適な実施形態においては、カット頂点セットは、最小のカット頂点セットより成る。

本発明の更に別の観点によれば、コンフィギュレーションドライバーは、受動的ノードにリンクされた能動的ノードに対してコンフィギュレーションデータを発生することにより受動的ノードのセキュリティポリシーを実施するためのリソースを含む。又、コンフィギュレーションドライバーのリソースは、トポロジー記憶装置のデータに基づいて実施できないセキュリティポリシーステートメントを識別する。

トポロジーデータ記憶装置は、１つの好ましい観点においては、セキュリティフレームワーク内に入るノードセット内の特定ノードに関する情報を与えるデータ構造体を含む。このデータ構造体は、ネットワーク層アドレス、MAC層アド

レス、上位層ユーザ識別子、搬送層のポート及びソケット番号、特定のノードがセキュリティポリシーを実施する信頼があるかどうか、ノードが実施できるセキュリティポリシーの形式、ポリシーを実施するのに使用される構造、セキュリティ構造に必要なコンフィギュレーションデータのフォーマット、及びノードとネットワーク内の他のノードとの接続のような情報を含む。

本発明の更に別の観点によれば、コンフィギュレーションドライバーは、ネットワークに分散されたセキュリティ機能のためのコンフィギュレーションデータを発生する。コンフィギュレーションデータは、永続的な記憶能力を有するコンフィギュレーション記憶装置に記憶され、これは、コンフィギュレーションデータに関連したノードセットにおける特定のノードと通信する。ネットワーク内のあるデバイスのコンフィギュレーション記憶装置は、例えば、不揮発性のプログラマブルメモリの形態でデバイス自体に含まれる。別のシステムでは、コンフィギュレーション記憶装置は、ポリシーが実施されるノード以外のネットワーク内のノードに設けられ、そして通信リンクによってポリシーが実施される特定のノードに接続される。本発明のこの観点によれば、コンフィギュレーションドライバーは、更新されたコンフィギュレーションデータをコンフィギュレーション記憶装置に送信し、その後、セキュリティ機能が実行されるノードに、記憶装置のコンフィギュレーションが更新されたことを通知する。このノードは、次いで、更新されたコンフィギュレーションデータを読み取り、そして更新されたポリシーの実行を開始する。

又、本発明は、より一般的には、ネットワークにファイアウオールシステムを確立する方法を特徴とすることができる。この方法は、ネットワーク内のノードにおいて動作するセキュリティ機能と、ネットワーク内のノードの相互接続とに関する情報を含むトポロジーデータを与えることを含む。次いで、この方法は、当該ノードの形式（1つ又は複数）に合致するフォーマット及び通信チャンネルを使用して、セキュリティ確保されたネットワーク内の最終システム間で実施されるべきセキュリティポリシーを含むセキュリティポリシーステートメントを与えることを含む。次いで、この方法は、トポロジーデータに応答して、セキュリティーポリシーステートメントを、ネットワーク内で動作するセキュリティ機能のためのコンフィギュレーションデータに変換することを含む。最終的に、この方法は、ノードの種々の形式に合致するフォーマット及び通信チャンネルを使用して、ネットワーク内の能動的なノードにおいてセキュリティ機能のコンフィギュレーションデータを確立することを含む。セキュリティ機能が1つの別の形態で動作するところの多数のプロトコル層は、少なくとも2つのプロトコル層、例えば、データリンク層、ネットワーク層、搬送層、並びにそのアプリケーション又は等効物の少なくとも2つを含む。

従って、本発明は、ネットワークインターフェイスカード、スイッチ、ルータ及びリモートアクセスシステムに設けられたセキュリティ機能の利点を取り入れ、

そしてファイアウオール機能をネットワーク内の種々のデバイスへと移動して、浸透した多層型ファイアウオールを形成する機会をシステムアドミニストレーターに与える。セキュリティ特徴は、多数のデバイスに対して多数の層に分散し、そしてコヒレントなセキュリテイポリシーマネージメントインターフェイスを用いて管理することができ、このインターフェイスは、ネットワークのセキュリティ特性を介して便利で且つ明確な制御をセキュリティアドミニストレーターに与える。分散された機能と、便利で且つ明確な制御は、分散型リモート監視ｄｒＭＯＮのようなシステム、又は単一目的機能に向けられた他の精巧なネットワークシステムに対してのみ現存するファイアウオールの利点を拡張できるようにする。

フィルタリングルール及び保護通信インフラストラクチャー情報セットのようなセキュリティポリシーデータを含むネットワークデバイスの数が増加するにつれて、コヒレントで且つ整合されたデータ管理を与えることが益々重要となる。本発明は、種々の多層ネットワークにおいてセキュリティポリシー実施データを管理及び分散するためのコヒレントな解決策を提供する。

本発明の他の特徴及び効果は、添付図面、その詳細な説明及び請求の範囲から明らかとなろう。

図面の簡単な説明

図１は、本発明による多層型ファイアウオールシステムを含むネットワークを示す簡単な図である。

図２は、本発明の多層型ファイアウオールシステムに含まれる種々のネットワーク要素を示す図である。

図３は、本発明による多層型ファイアウオールを実施するプロセスを示すフローチャートである。

図４は、本発明による多層型ファイアウオール機能を実施するための別の技術を示すフローチャートである。

図５は、本発明の多層型ファイアウオールシステムによりネットワーク内のノードにコンフィギュレーションデータを確立するのに含まれる段階を示すフローチャートである。

図６及び７は、図２の変形であって、本発明による例示的なセキュリティフレームワークを強調して示した図である。

好ましい実施形態の詳細な説明

先ず、図１ないし５を参照して本発明を詳細に説明する。図１は、概観図である。

図１において、ネットワーク１０は複数のノードを含む。ネットワーク内の少なくとも１つのノードは、ネットワークマネージメントステーション１１又は他のセキュリティポリシーサーバを含む。ネットワーク内の他のノードは、スイッチ１２と、リモートアクセス装置１３と、ルータ１４と、ネットワークインターフェイスカード及びそれをサポートするドライバーソフトウェを含む最終ステーション１５と、中継器１６とを備えている。従って、ネットワーク１０には種々のネットワークデバイスが含まれる。スイッチ１２、リモートアクセス装置１３、ルータ１４、最終ステーションのネットワークインターフェイスカード１５及び中継器１６は、全て、セキュリティポリシーマネージメントエージェント２２、２３、２４、２５及び２６を各々含む。これらセキュリティポリシーマネージメントエージェント２２－２６は、種々のプロトコル層においてセキュリティ機

能を実行する。エージェントが実施される特定のネットワークデバイスを横断するプロトコル層と、他の構造的特徴とに基づいて、セキュリティ機能に使用される構造は、デバイス形式ごとに変化する。

図１に示す実施形態では、ネットワークマネージメントステーション１１は、トポロジーデータ記憶装置３０と、コンフィギュレーションインターフェイスの前端３１と、コンフィギュレーションドライバーを構成するセキュリティポリシーマネージメント後端３２とを備えている。トポロジーデータ記憶装置３０は、ネットワークのノードにおいて多数のプロトコル層で動作するセキュリティポリシーマネージメントエージェント２２－２６２より実行されるセキュリティ機能に関する情報を記憶する。又、このトポロジーデータベースは、ネットワークにおけるノードの相互接続も指示する。

コンフィギュレーションインターフェイスの前端３１は、トポロジーデータベース３０に接続される。これは、セキュリティポリシーステートメントを受け取るための入力を含み、例えば、セキュリティポリシー言語のスクリプトを与え、

このスクリプトをインタープリター３４により解読して、セキュリティポリシーステートメントを形成する。セキュリティポリシーマネージメントの後端３２は、コンフィギュレーションインターフェイスの前端３１及びトポロジーデータベース３０に接続され、セキュリティポリシーステートメントをネットワーク内のノードのコンフィギュレーションデータへと変換するリソースを含む。セキュリティポリシーマネージメントの後端３２は、セキュリティポリシーステートメントを実施すべきネットワーク内のノードにおいてセキュリティポリシーマネージメントエージェント２２－２６へのコンフィギュレーションデータを確立するコンフィギュレーションドライバーを構成する。

コンフィギュレーションインターフェイスの前端３１は、１つの実施形態においては、セキュリティポリシー言語のスクリプトをシステムに入力するところのテキスト入力デバイスを含む。別の実施形態では、コンフィギュレーションシステムインターフェイスの前端３１は、ユーザがセキュリティポリシーステートメントを特定するところのグラフィックユーザインターフェイスを含む。各々の解

決策において、セキュリティポリシーステートメントを、そのポリシーが実施されるネットワーク内のノードの適当なプロトコルレベル及びデバイス形式に対するコンフィギュレーションデータへと変換することのできるシンタックスを有するセキュリティポリシースクリプトが与えられる。

セキュリティポリシー言語及びセキュリティポリシー言語前端

セキュリティポリシー言語は、ネットワーク内のアクティビティに対する制約を特定するのに使用される。このようなアクティビティは、中継器、スイッチ、ルータ、リモートアクセス装置等のネットワークデバイスと、ネットワークの最終システムとの両方によって行なわれるアクティビティを含む。多層ファイアウオールは、特定の設備に適したセキュリティポリシー言語で実施できるが、1つの言語を以下に例示する。

各最終システム及び能動的ネットワークデバイスは、そのセキュリティポリシーマネージメントエージェントに関連した1つ以上のネットワークアドレスを有し、そして1つ以上の他のネットワークデバイスに接続される。この情報は、セキュリティポリシー言語前端によりシステムアドミニストレータとの対話を介して得られると共に、トポロジーデータベースから得られる。システムアドミニストレータとの対話は、ユーザインターフェイスを経て行なわれるか、或いはファイルや他の記憶リソース、例えば、ドメインネームシステム(DNS)、ネットワークインフォメーションサービス(NIS)又は他のベースの読み取りによって行なわれる。最終システムは、それらが常にトポロジーデータベースから形成されたグラフに放置されるという点でネットワークデバイスとは区別される。「ノード」という一般的な表現は、最終システム又はネットワークデバイスのいずれかを指す。最終システム(aka ホスト)は、ポリシーステートメントにおいて識別されるノードである。例えば、管理の目的でネットワークデバイスがアクセスされるときには特殊なケースが生じる。このケースでは、ネットワークデバイスが最終システムの役割を果たす。

ネットワークの最終システムは、グループに属してもよい。グループは、名前が付けられ、そしてそれらのメンバーシップは、システムアドミニストレータ等

によるか又はトポロジーデータベースで実施される別の形態においてセキュリティポリシー言語前端への入力で確立される。この場合も、この入力は、ユーザインターフェイスの対話によるか、又はセキュリティポリシー言語前端がファイル又は他のデータベースを読み取ることにより得ることができる。最終システムのグループは、個々の最終システム又は最終システムの他のグループを含むものとして特定されてもよい。最終的に、通信リンクを経て、セキュリティが適用されるネットワークの外部の他のノードへ接続されるノードは、トポロジーデータベースに記入される。1つの実施形態において、シンタックスは、多層ファイアウオールのマネージメントドメイン以外の最終システムを表わす「外部」という名前の特殊な「仮想」ノードを与える。従って、トポロジーは、そのトポロジーにおける特定のノードが特殊なノード「外部」に接続されたかどうかを指示する。別の実施形態では、名前の付いた外部ノードが2つ以上存在することも考えられる。これは、多層ファイアウオールが、2つ以上の他の外部多層ファイアウオールと通信するためのポリシーを定義できるようにする。

又、セキュリティポリシー言語前端は、他の情報、例えば、ユーザ識別子、ユーザ識別子のグループ、行先へのアクセスがソースによって許される時間長さに対する時間仕様、行先へのアクセスが許される時間間隔の仕様、等々を管理し、又はそれらを特定する前端として働くのが好ましい。

セキュリティポリシー言語それ自体は、ネットワーク内の最終システム間に許されたアクティビティを特定するセキュリティポリシーステートメントのセットを書き込むのに使用される。例示的なルールベース及びシンタックスは、次の通りである。

ソース	行先	アクティビティ	ポリシーステートメント	実施場所
ホスト1	ホスト2	FTP	「ジョン・ドゥ」と「ジェーン・ディア」の従業員に対し月曜ー金曜の午前5時から午後7時まで許す	行先
ホスト3	ホストグループ1	テルネット	不許可	行先
ホストグループ1	ホストグループ2	真の音声	月曜ー金曜の午前5時から午後8時まで許す	両方
ホストグループ2	ホスト1	HTTP	許可；オーデット	行先
外部	ホスト又はホストグループ	HTTP	許可	ソース
ホスト又はホストグループ	外部	FTP	許可	ソース

トポロジー情報データベース

トポロジー情報データベースは、ノード及びそれらがいかに相互接続されたかに関する情報を含む。ノードに特有の情報は、1つの例では、そのネットワークアドレス（1つ又は複数）と、そのMACアドレス（1つ又は複数）と、その許された関連ユーザ識別子と、そのポート又はソケット番号と、セキュリティポリシーを実施する信頼があるかどうかと、実施できるのはどんな形式の実施ルールかと、ノードにおけるセキュリティ構造のフォーマットと、ネットワークにおけるノード間の相互接続とを含む。

ノードがいかに接続されるかの情報は、各ノード又はノードネットワークインターフェイスの識別子と、どのノードがどのノードインターフェイスを経て他のどのノードに直接接続されるかを特定するグラフ情報とを含む。又、この情報は、「外部」ノード、或いは外部接続を指示する別のファイアウオールシステム又は別のデータ構造体に接続されたノードも含む。1つの拡張において、情報は、物

理的ノード内の個々のプロセスを識別する。

トポロジーデータベースは、一例において、単一のデータベースマネージメントシステムによって管理されるか、或いは個々のノード又はノードの集合においてデータベース前端システムにより管理される多数のデータベースから構成される。多数のデータベースにおけるデータは、例えば、RMON及びdRMONデータと、最終システム及びネットワークデバイスにより管理されるセキュリティ情報と、ネットワークを通して分散されたネットワークマネージメントシステムにより得られる接続情報とを含む。

セキュリティポリシーマネージメント後端

セキュリティポリシーマネージメント後端は、セキュリティポリシー前端コンフィギュレーションインターフェイス及びトポロジーデータベースからの情報を使用して、セキュリティポリシーステートメントにより特定されたセキュリティポリシーを形成、記憶、更新、分配及び実施する。後端は、スタンドアローンマネージメントシステム、永続的記憶システム及びノードにおけるエレメントより成る。セキュリティポリシーマネージメント後端は、トポロジーデータベースにおける情報のコンテクストにおいてセキュリティポリシーステートメントで特定されたルールを変換し、そしてノード特有のセキュリティポリシーコンフィギュレーションデータを構成し、それが選択したネットワークノードへ分配する。セキュリティポリシーマネージメント後端は、セキュリティポリシーステートメントを、特定のノードで実施できるコンフィギュレーションデータのセットにいかに区画化するかを判断し、そしてセキュリティポリシーステートメントのルールを、その選択されたノードで実施できるノード特有のコンフィギュレーションデータへと変換する。

ノード特有のセキュリティポリシーコンフィギュレーションデータは、ノードのフィルタリングエンジンを駆動するフィルタリングルールのような静的なデータを含むか、又はジャバ、ソース又はバイトコードのような動的なデータリンクプログラムや、TCL、ピアール、Cシェルスクリプトのようなスクリプト言語で表わされたプログラムを含む。特定のノードで実施されるセキュリティポリシ

ーステートメントを表すコンフィギュレーションデータのフォーマットは、特定のノード及びそのセキュリティポリシー実施エージェントに基づく。

1つの別の形態において、セキュリティポリシーマネージメント後端は、セキュリティポリシーステートメントが上記のシンタックスに基づいて表わされると仮定すれば、セキュリティポリシーステートメント及びトポロジーデータベース情報を分析して、次のプロセスに基づきデバイス特有のセキュリティポリシーコンフィギュレーションデータを駆動する。

1．ノードは、2つの分類に分けられる。1）ポリシーを実施できないか又は実施する信頼性がないためにポリシーを実施することのできない受動的ノード、及び2）ポリシーを実施することのできる能動的ノード。

2．各能動的ノードごとに、それに直結されるか、又は受動的ノードから他の受動的ノードを経て能動的ノードへ至る経路が存在するところの全ての受動的ノードのリストを形成する。このリストにおける各受動的ノードは、能動的ノードの関連ノードと称される。

3．各セキュリティポリシールールに対して、ソースノードのセットを形成し（即ちリストが個々のノードのみを含むまでソースセットにおけるノードの全グループを繰り返し拡張することにより）、そして行先ノードのセットを決定する（ソースセットにおけるノードではなく行先セットにおけるノードを使用すること以外は同じ分解アルゴリズムを使用して）。

4．各セキュリティポリシールールに対して、次の計算を実行する。ソースノードセットにおける各受動的ノードごとに、そこから、能動的ノードを横断しない行先ノードセットの受動的ノードへ至る経路が存在するかどうか決定する。もしそうであれば、ルールを実施できないことを通知する。

5．ルールが、ソースにおいて実施すべきであることを特定する場合には、

- ソースノードセットにおいて関連ノードを伴う能動的ノードのセットを決定する。
- これら能動的ノードの各々に対し、ルールで特定されたセキュリティポリシーステートメントを、ノードが実施できるセキュリティポリシーコンフィギュレーションデータ、即ちそれ自身のセキュリティポリシー言語のルールへと変換する。
- ノード特有の通信チャンネルを使用してノードにおいてこれらルールを確立する。

6．ルールが、行先ノードセットにおいて実施すべきであることを特定する場合には、

- 行先ノードセットにおける関連ノードを使用する以外は、上記5の場合と同じことを行う。

7．ルールが、ソースノードセット及び行先ノードセットの両方において実施すべきことを特定する場合には、

- 上記5及び6の両方を行う。

上述したルールに基づくセキュリティポリシーの実施は、図2及び3を参照して良く理解することができよう。図2は、本発明によるセキュリティポリシーが多数の層において実施されるネットワークの要素を詳細に例示する。図3は、分散型多層ファイアウオールの実施を示す全体的なフローチャートである。

図2から明らかなように、代表的なネットワークは、種々様々なネットワークデバイス及び最終システムを備えている。従って、図2は、ノードのセットを含むネットワークを示し、ノードセットにおけるノードは、多数のプロトコル層にセキュリティ機能を与える。ネットワークは、汎用のワイドエリアネットワークWANファシリティ100を備えている。ワイドエリアネットワーク100は、第1のプライベートネットワーク101及び第2のプライベートネットワーク102に接続される。第1のプライベートネットワーク101の要素は詳細に示されているが、第2のプライベートネットワーク102は雲の形で示されている。又、ワイドエリアネットワークファシリティ100は、スタンドアローンのルータ型の最終システム103と、公衆交換電話ネットワーク（PSTN）105に接続されたラインサーバ104と、これもPSTN105に接続されたアクセスサーバ106とに接続される。図2に示すように、WANファシリティ100は、サイトルータ107、パケットサーバ108及び別のサイトルータ109を経

てプライベートネットワーク１０１に接続される。

ＰＳＴＮ１０５は、モデム１１０を経てスタンドアローンのダイアルアップ最終システム１１１に接続される。又、ＰＳＴＮ１０５は、リモートアクセスルータ１１２に接続される。リモートアクセスルータ１１２は、最終システム１１３及び１１４に接続される。又、リモートアクセスルータ１１２は、ターミナルサーバ１１５に接続され、これは、次いで、最終システム１１６及び１１７に接続される。

第１のプライベートネットワーク１０１において、パケットサーバ１０８は、この例では中継器又はスイッチの機能を与えるハブ１２０に接続される。ハブは、次いで、サイトルータ１０７及びサイトルータ１０９に接続される。サイトルータ１０７、１０９の各々は、ワイドエリアネットワークファシリティ１００にも接続される。サイトルータ１０７は、アクセスサーバ１２１に接続され、これは、ＰＳＴＮ１０５に接続される。又、サイトルータ１０７は、スイッチ１２２及びスイッチ１２３を含むスイッチセットに接続される。サイトルータ１０９は、スイッチ１２４に接続される。スイッチ１２４は、中継器１２５で表わされた中継器セットに接続される。中継器１２５は、図１のノード１１に対応するセキュリティポリシーマネージメントリソースを含む最終ステーション１２６に接続される。

又、プライベートネットワーク１０１は、スイッチ１２２及び１２３に接続された要素で表わされた多数の他のデバイスも含む。スイッチ１２２は、中継器１３０及び最終システム１３１のネットワークインターフェイスカードＮＩＣへの接続を含む構成で示されている。中継器１３０は、ネットワークインターフェイスカードを含む最終システム１３２を備えた最終システムセットにも接続される。

スイッチ１２３は、中継器１３３に接続され、これは、次いで、最終システム１３４を含む多数の最終システムに接続される。スイッチ１２３は、図中雲の形で一般的に示されたスイッチネットワーク１４０に接続される。スイッチネットワーク１４０は、スイッチ１４１に接続される。スイッチ１４１は、中継器１４２に接続され、これは、次いで、ネットワークインターフェイスカードＮＩＣを含む最終システム１４３に接続される。

図２において、セキュリティポリシー実施エージェントが配置されたノードは、水平のバーでコード化される。従って、図の左上の隅から始めて、モデム１１０、リモートアクセスルータ１１２、ターミナルサーバ１１５、アクセスサーバ１０６、ラインサーバ１０４、パケットサーバ１０８、サイトルータ１０７、サイトルータ１０９、スイッチ１２２、スイッチ１２３、中継器１３３、及び最終システム１３１、１３２のネットワークインターフェイスカードは、全て、セキュリティポリシーを実施するエージェントを含む。ポリシーマネージメントステーション１２６は、上述したコンフィギュレーションインターフェイス、トポロジーデータベース、及びコンフィギュレーションドライバ後端を形成するリソースを備えている。

本発明に基づいてセキュリティポリシーを実施できる典型的なネットワークにおけるデバイスの概要を以下に説明する。次いで、図３－６を参照して、本発明のプロセス全体を説明する。

ネットワークインターフェイスカード及びモデム

ノードセットにおける最も基本的な製品は、ネットワークインターフェイスカード（ＮＩＣ）及びモデムである。ＮＩＣは、内部Ｉ／Ｏバスを経て最終システムに取り付けられて、イーサネット、高速イーサネット、ギガビットイーサネット、トークンリング、ＦＤＤＩ及びＡＴＭのようなローカルエリアネットワークへの最終システムアクセスを与えるＩ／Ｏデバイスである。ＡＴＭの場合には、あるＮＩＣは、ＡＴＭのワイドエリアネットワークにアクセスすることができる。

モデムは、シリアル又はパラレルインターフェイスを経て最終システムに取り付けられる外部装置である。一般に、それらは、最終システムがＰＳＴＮ又は非交換式の地上ラインを使用してデータを移動できるようにする。

従来、ＮＩＣ及びモデムは、特徴ではなくて性能に対して最適化された簡単な装置である。

おそらく、広範囲な受け入れを得るための第1のＮＩＣセキュリティ特徴は、ＮＩＣブートＲＯＭである。ネットワークサーバからディスクなしでブートできるように最初に意図されたブートＲＯＭは、信頼性のあるブートコードの実行を保証するという関心のあるセキュリティ副作用を有する。ある支援ソフトウェアと共にこれを使用して、信頼性のあるコードを最終システムへロードし、このシステムがＮＩＣを確実に動作するよう構成する。

セキュリティの実施と共に益々普及した特徴は、フィルタリングである。フィルタリングの使用は、多数の目的により動機付けされる。ＬＡＮレベルにおいてフィルタリングを使用して、フレームの無制限な送信から生じるリソース欠乏の問題からＮＩＣ及びハブが保護される。この形式のフィルタリングを与えるために開発された構造は、ＶＬＡＮとして知られている。層2より上で動作するより一般的な機構は、ルータを横切ってフィルタリングを行えるようにする。これらの機構は、ＶＮＥＴとして一般に知られている。

フィルタリングをセキュリティの目的に使用することは、ＮＩＣ、スイッチ、中継器、ルータ及びリモートアクセス装置で行うことができる。ＮＩＣ内でのフィルタリングは、それが送信するソースＭＡＣアドレスが有効であることを保証すると共に、それが受信するソースアドレスが信頼性のある最終システムからのものであることを保証するようために使用できる。しかしながら、ＮＩＣフィルタリングは、他の等しく有効な目的にも使用でき、例えば、ハブからＶＬＡＮの実行処理の負荷を除去し、浸透した多層ファイアウオールを実施し、そして高レベルセキュリティプロトコルに対するハードウェアサポートを与えるのに使用できる。

ＮＩＣ及びモデムにとって独特の1つの保護通信特徴は、ある物理的な通信チャンネルによって与えられる高レベルの流出セキュリティである。特に、光ファイバラインの使用は、侵入者による受動的な盗聴のおそれを低減する。

更に、多くの顧客は、彼等の内部ネットワークが、通信ポート及び最終システムへの物理的なアクセスを得ようとする侵入者に対して益々抵抗力のない状態になりつつある。例えば、慎重さを要する資産的情報を保持する会社のイントラネットは、広い地域にわたって延びていて、遠隔のエンジニアリング及びセールス

オフィスがそれらに接続されている。これらの遠隔オフィスは、典型的な会社の構内に見られる同じレベルの物理的セキュリティを与えるものではない。

ＮＩＣ及びモデムは、両方ともネットワークアクセス制御をサポートする特徴を与えることができる。モデムは、出ダイヤルシーケンスを実行する前に、ユーザがパスワードを与え、トークンカードを使用し、又はさもなくば、接続を開始することが許されたという証拠を示すことを必要とする。又、モデムは、許可された電話番号からの接続だけを許すアクセスサーバにおいてコールバック機能をサポートすることもできる。

セキュリティポリシーの後端は、例えば、更新されたＮＩＣブートコードを関連ネットワークサーバに記憶し、そしてＮＩＣに再ブートするよう通知することにより、ＮＩＣにセキュリティルールを確立する。モデムにおいては、ドライバーコードが更新されるか、又はモデムマネージメントコードとの通信により新たな値がコンフィギュレーションレジスタに書き込まれる。

中継器

ハブは、他の最終システムにフレームを送信しそしてプロトコルハイアラーキーの層2に接続を与えるためにＮＩＣが接続されるスターネットワーク装置である。ハブを相互接続して相互接続ツリーを形成することによりハイアラーキーネットワークを構築することができそしてそのようにするのが一般的である。

中継器は、それが受信したフレームをそれらの全てのライン（フレームが到着したラインを除いて）に放送するハブである。中継器は、低廉な相互接続組織を構築するのに有用である。しかしながら、相互接続された中継器の数が増加するにつれて、接続された最終システム間の干渉も増加する。それ故、中継器を使用して直接接続できる最終システムの数には限度がある。

中継器は、一般にコストを減少するために特徴を最小限に抑える基本的な放送デバイスである。しかしながら、それらにおいてセキュリティ特徴が実施されている。

層2における保護通信は、本来セキュリティに問題があるが、中継器によって少なくとも部分的に対処することができる。とりわけ、ある中継器は、フレームがアドレスされないセグメントにわたって放送されたフレーム内のデータを歪曲

する。これは、これらセグメントに取り付けられた探知機がこれらフレーム内のデータを見ることができないよう確保すると共に、衝突検出アルゴリズムが適切に働き続けるよう保証する。

高端中継器は、ＩＥＥＥ８０２．１０規格で定義されたような精巧な保護通信機構又はあまり複雑でない他の機構を実施することができる。このような機構は、フレームに保持されるデータを保護するために暗号化技術を使用する。このような保護は、浸透した多層ファイアウオール及びネットワークアクセス制御機構のようなシステムセキュリティ特徴を実施しそして最終システムデータの保護を与えるのに有用である。

従って、セキュリティポリシー後端は、隣接マネージメントノード又はマネージメントリソースを中継器自身において更新することにより中継器にコンフィギュレーションデータを確立する。

スイッチ

スイッチは、フレームのソース及び行先アドレス（並びにおそらくは他の情報）を検査して、それらのラインのどれを使用して受信フレームを転送すべきか決定するハブである。中継器に勝るスイッチの利点は、行先への経路上にあるラインのみを経てフレームを送信することにより最終システムへのトラフィックを減少することである。放送されたフレームの場合には、スイッチは、スイッチ内に保持されたポリシー情報に基づきあるラインを経てそれらを中継しないように決定することができる。

ＡＴＭ、イーサネット、高速イーサネット及びトークンリングスイッチを含む種々の能力及びコストのスイッチが製造される。ＡＴＭスイッチは、他のＲＡＮ形式に対して作られたスイッチより著しく複雑である。特に、ＡＴＭスイッチが相互接続されるときには、スイッチが最終システム間に確立した仮想回路を経てフレームを移動する。これは、最終システムからスイッチへ及びスイッチ間での制御情報の移動を必要とする。この形式のトラフィックは、他のアクセス技術のスイッチでは必要とされない。

又、中継器により実施される全ての機能は、スイッチでも実施できる（前記の説明を参照）。加えて、スイッチは、種々のフィルタリング機能を実行するのに適した場所である。あるスイッチは、ＶＬＡＮサポートの形態でこれを既に行うことができる。セキュリティを与えるのに加えて、ＶＬＡＮは、ＶＬＡＮメンバーのないセグメントを経てフレームが放送されるのを阻止することによりスイッチ／中継器通信組織に流れるトラフィックの量を減少する。

フィルタリング機構は、従来、フィルタリングが適用されるフレームの種々の特性に基づいて受け入れ判断を行う。しかしながら、フレームの制御及び／又はデータを変換するというフィルタリングのより精巧な使い方がある。例えば、浸透した多層ファイアウオールを実施するには、フレームを別の保護フレーム内にカプセル化し、層２のセキュリティトンネルを実施することが必要となる。層２のトンネルは、ＡＴＭスイッチ（ＬＡＮエミュレーション）と、ＬＡＮトラフィック搬送ＡＴＭセル（ＣＩＦ）とによって既に実施されている。セキュリティトンネルの概念は、トンネル媒体を通過するときにトンネルトラフィックを保護することによりこれらの機構を拡張する。変換フィルタリングの別の分類は、層２アドレス変換であり、これは、浸透したファイアウオールの実施に有用である。

スイッチは、ＲＡＤＩＵＳ、ＴＡＣＡＣＳ＋及びネットウェアＮＤＳのような認証、許可及びオーデット（ＡＡＡ）サーバとの代理対話のようなヘッド端ネットワークアクセス制御機能を入れるための本来の場所である。スイッチは、中継器に関連して、ポートの切断及び再接続を監視し、これらをネットワークマネージメントアプリケーションに報告することができる。

又、スイッチは、セキュリティ支援特徴を入れるための便利な場所でもある。例えば、スイッチは、信頼のあるサーバのみがブート像を最終システムへ供給するよう確保するためにシステム認証プロトコルを実施することができる。スイッチは、承認ハイアラーキーの最上位の公開キーを含む公開キー暗号化に使用されるトップレベル承認のようなあるセキュリティーインフラストラクチャー情報を保持しそして分配することができる。

セキュリティポリシー後端は、スイッチにおいて実施されるＳＮＭＰのようなマネージメント通信チャンネルを使用するか、又はアプリケーション層のピアーピア通信プロトコルを使用してスイッチのセキュリティ構造を更新する。

ルータ

ルータは、それらのインターフェイス間でパケットを移動し、これらパケットをソースと行先との間で進行させるための装置である。ルート指定の判断は、通常、パケットのソース及び行先ネットワーク層アドレス、及び他の情報（例えば、パケットのサービスクオリティ、セキュリティオプションデータ及びホップカウント）に基づく。ルータは、次のことを含む多数の特性によりスイッチから区別される。即ち、1）ルータは、異なるアクセス媒体に接続されたインターフェイス間でデータを移動し、2）層2制御情報に基づくのではなく、層3パケットに保持された情報に基づいてルート指定を行い、そして3）通常フレームを全てのインターフェイスに放送しない。

しかしながら、ネットワーク業界における最近の傾向は、スイッチング及びルート指定を同じネットワークデバイスに一体化することである。多数のネットワーク会社は、異なるアクセス媒体フレームフォーマット間を切り換えるスイッチを製造し、従って、これらスイッチは、異なるアクセス技術に接続されたインターフェイス間でデータを移動することができる。更に、ＩＰマルチキャストのような層3放送プロトコルが益々普及してきている。その結果、ルータは、現在、スイッチに非常に類似した放送機能を遂行する。従って、ルータとスイッチとの間に残された1つの重要な区別は、その機能を遂行するためにその情報を得る場所（プロトコル層）であると考えられる。

ルータとスイッチとの相違がこのように緩和したのに加えて、同じ装置でルート指定及びスイッチングの両方を遂行する多数の会社の製品が市場に出回っている。これについて特に注目すべきは、トラフィックパターンを追跡してＩＰパケットをルート指定するカリフォルニア州、サニーベールのイプシロンネットワークス社のルータ／スイッチである。特定のソースと行先との間のトラフィックが特定のスレッシュホールドに到達した場合には、ルータは、これらシステム間のパケットが比較的高価なＩＰルート指定プロセスをバイパスできるようにするカットスルー層2接続を設定する。

ルータは、スイッチと同じ多数のセキュリティサービスを与えるが、プロトコルハイアラーキーの層3ではこれを行なわない。層3の保護通信特徴を定義する

現在の活動は非常に多数ある。この活動は、ＩＥＴＦのＩＰＳＥＣワーキンググループを中心とする。ＩＰＳＥＣは、公表されると共に開発中である1組の規格であって、最終システム及びルータがＩＰプロトコルに対して認証、完全性及び機密性サービスをいかに提供するかを規定する。このようなサービスを利用し、端ー端保護と、中間ルータ間及びルータと最終システムとの間のトンネルの保護との両方を与えることができる。

又、ルータにより与えられる従来のフィルタリングサービスは、それらがファイアウオールの要素として働くことができるようにする。一般に、ファイアウオールは、ネットワーク層、搬送層及びアプリケーション層におけるパケットフイルタリングと、アプリケーション代行との2つの機能を遂行する。ルータは、一般に、最初のサービスしか与えない。しかしながら、ファイアウオール技術は、ルータ内に状態マシンを設けて、ＦＴＰ制御トラフィック及びＴＣＰ接続開放パケットのような、それを通して転送されるパケットを追跡し、そしてこの保持された状態を使用して、フィルタリングプロセスを推し進めるという傾向である。この特徴は、パケットフィルタリングとアプリケーション代行との間の区別を不明瞭にする。

フィルタリングを適切に使用すると、顧客は、仮想ネットワーク（ＶＮＥＴ）を実施することができる。ＶＮＥＴは、ＶＬＡＮの層3等効物である。それらは、層3の通信組織を経て移動されたトラフィックを個別のドメインに分離する。ＶＮＥＴに属さない最終システム及びＬＡＮセグメントには、そのトラフィックが見えない。

セキュリティポリシー後端とルータとの間の通信は、通常、アプリケーション層におけるピアーピア通信である。もちろん、ＳＮＭＰのようなマネージメントチャンネルを使用することができる。

リモートアクセス装置

リモートアクセス装置は、シリアルラインを経て送られる通信を、ルート指定されたトラフィックに変換する。更に、それらは、ＳＰＸキープ・アライブ、ローカルノードエミュレーション、等のプロトコル代理処理をサポートする。

最終システムは、リモートアクセス装置（例えば、ターミナルサーバ）に直結

することもできるし、又は公衆交換電話ネットワーク（ＰＳＴＮ）を経て接続することもできる。より一般的な状態は、ＰＳＴＮを通る接続であり、これは、アクセスサーバの使用を必要とする。

アクセスサーバ装置には２つの主たる使用目的がある。その第１は、プライベートイントラネットへのリモートアクセスを与えることである。この場合、アクセスサーバは、プライベートイントラネット内に配置され、スタンドアローンの最終システム及びリモートオフィスルータがＰＳＴＮを経てリモートアクセスできるようにする。リモートアクセス製品の第２の使用目的は、インターネットサービスプロバイダー（ＩＳＰ）ネットワーク内である。これらは、ＩＳＰの包含装置及びＩＳＰのインターネット接続への加入者アクセスを与える。これら２つの使用目的は、若干異なるセキュリティ要求を有し、これについて以下に詳細に述べる。

リモートアクセス装置の２つの機能、即ちラインサービス及びパケット処理は、従来、同じシャーシ内で実施されている。最近の顧客要求の変化、特に、公衆ＷＡＮを使用してプライベート仮想ネットワークを実施するという要望に伴い、売主は、これらの機能を、ラインサーバ及びパケットサーバの２つの異なる製品に分離するようになった。顧客がこれらの製品を使用するときには、ラインサーバは、一方の側では、ＰＳＴＮに接続され(又はおそらく最終システムに直接接続され)、そして他方の側では、ＷＡＮに接続される。パケットサーバは、一方の側では、プライベートイントラネット又はＩＳＰファシリティに接続され、そして他方の側では、ＷＡＮに接続される。各接続に対して、ラインサーバは、ＷＡＮを通して（通常、暗号化技術を使用して）パケットサーバへ至る保護トンネルを形成する。ラインサーバへの接続は、スタンドアローンの最終システム又はリモートオフィスのルータ装置から到来する。

３つのリモートアクセスコンフィギュレーションが代表的である。

第１のＷＡＮアクセスは、公衆交換電話ネットワーク（ＰＳＴＮ）を経てそれらの内部リソース及びインターネットへのアクセスを与えるためにＩＳＰにより使用される。アクセスサーバがＰＳＴＮに接続され、スタンドアローンの最終システムをもつクライアントに接続することができる。

第２は、リモートオフィス及びテレコミュニケーション装置にプライベートネットワークへのアクセスを与えるリモートオフィスアクセスコンフイギュレーションである。リモートアクセスルータは、ＰＳＴＮを使用して、会社の構内又は他の組織のアクセスサーバに接続する。アクセスサーバは、次いで、リモートアクセスルータからプライベートイントラネットへネットワークトラフィックを転送する。

第３のコンフィギュレーション、即ちスプリットサーバアクセスは、ラインサーバ及びパケットサーバ機能を個別の装置に分離する。ラインサーバは、シリアルラインマネージメント及びデータ通信問題を取り扱い、一方、パケットサーバは、ＷＡＮとプライベートイントラネットとの間のインターフェイスを取り扱う。

３つのコンフィギュレーションは、全て、ある種のネットワークアクセス制御を必要とする。ＷＡＮアクセスの場合には、ＷＡＮへのアクセスを与える前に、ユーザを認証しそして許可を与える。インターネットアクセスに加えて、ローカルリソース（例えば、ローカルで管理される内容、ｅ－メールサービス、ウェブページ）へのアクセスも与えるＩＳＰも、ユーザがローカルリソースを使用できる前に、ユーザを認証しそして許可を与える。

リモートオフィスアクセスは、プライベートイントラネットを経てトラフィックを流せる前に、リモートオフィスを認証しそして許可を与えることを必要とする。ルータは、それ自体、ユーザを代表するものでないので、初期の接続シーケンス中に認証及び許可を与えねばならない。通常、これは、ユーザ(システムアドミニストレータの役割を果たす)がリモートアクセス装置に対して認証を行い、そしてこの装置が、認証チェックを遂行した後に、プライベートイントラネットへの経路を開くことを必要とする。

スプリットサービスアクセスは、２つのネットワークアクセス制御判断を必要とする。その第１は、ラインサーバへのユーザアクセスを許し、そしてその第２は、パケットサーバ、ひいては、プライベートイントラネットへのユーザアクセスを許すことである。二重ログインでユーザに負担をかけるのを回避するために、スプリットサービスアクセスに使用されるネットワーク機構は、パケットサー

バ又はプライベートイントラネットにより管理されたアクセス制御リソースを使用

して、ラインサーバへユーザを入れることができる。このような場合に、ラインサーバとパケットサーバ/プライベートイントラネットは、両サーバへのユーザの入場を許可するように協働する。

リモートアクセスにとって重要な別のセキュリティサービスは、フィルタリングである。アクセスサーバ（一体的コンフィギュレーション又はスプリットコンフィギュレーションのいずれか）は、ファイアウオール機能を入れるための本来のポイントである。これは、2つの形式の一方をとることができる。最も簡単なものは、アクセスサーバ及びパケットサーバ（スプリットサービスアクセスの場合に）において従来のファイアウオールパケットフィルタリングを行うことである。このようなフィルタリングルールは、装置を通過する全てのトラフィックに適用される。

より進歩したフィルタリング形式は、接続ごとのベースで適用されるフイルタリングルールを確立することである。即ち、ユーザがアクセスサーバを経て接続を確立するときに、そのユーザに特有の1組のフィルタリングルールがフィルタリングデータベースから引き出される。これらルールは、次いで、アクセスサーバにインストールされ、アクセスサーバは、その接続を経て進行するトラフィックのみにそれを適用する。

更に、保護通信は、リモートアクセスによって与えられる重要なサービスである。これは、2つの段階で行なわれる。ある状態においては、ＰＳＴＮによって与えられる物理的なセキュリティでは、ユーザ/プライベートイントラネットに適切な保証を与えるのに不充分である。このような場合に、モデム/リモートアクセスルータは、アクセス/ラインサーバとの通信を暗号技術で保護することができる。これは、シリアルラインにわたって実行される暗号プロトコルを必要とする。

より一般的なケースは、ＷＡＮにわたる通信を保護する必要性から生じる。この状態においては、ＷＡＮにわたりシリアルライントラフィックを移動するのに

必要なトンネルプロトコルが暗号化によって保護される。これは、トンネルプロトコル内でのセキュリティサポートの結果として生じるか、又はＷＡＮに使用されるネットワークプロトコルにより与えられるセキュリティ特徴を使用する結果として生じる。後者の重要な例は、ＩＰＳＥＣを使用して、ＩＰ　ＷＡＮの通信を保護し、これにより、仮想プライベートネットワークを形成することである。

ネットワークマネージメント

実質上全てのネットワーク中間システム及びＮＩＣは、あるやり方で構成されるか、さもなくば、管理されねばらない。一般に、これは、簡単なネットワークマネージメントプロトコル（ＳＮＭＰ）を介して遂行され、これは、管理される各デバイスがリモートマネージメントソフトウェアにより制御されるエージェント機能を実施することを仮定する。通常、多数のエージェントが所与のマネージメントステーションにより管理される。

ネットワークデバイスは、通常、ＳＮＭＰマネージャーからの「ゲット・アンド・セット」要求に応答するＳＮＭＰエージェントを構成し、これは、サイトアドミニストレーターが、デバイスごとではなく一体化されたシステムの観点からネットワーク装置を管理できるようにする。

あるネットワークマネージメントシステムの1つの重要な特性は、分散型リモート監視（ｄＲＭＯＮ）を与えることである。リモート監視は、ＬＡＮ装置に接続された「プローブ」から統計学的情報及びアラーム情報をネットワークマネージャーに与える。しかしながら、ＬＡＮセグメントの数が増加するにつれて、プローブのリソースがその能力を越えてストレスを受け、不完全な情報がマネージメントステーションソフトウェアに送られることになる。この問題に対処するために、ｄＲＭＯＮは、プローブ機能の若干をＮＩＣ及びハブに分配し、これは、ＬＡＮのサイズが成長するにつれてリモート監視機能を拡張できるようにする。

2つのネットワークマネージメントの問題は、重要なセキュリティの観点によって特徴付けされる。その第1は、ネットワークマネージメントセキュリティであり、即ちネットワークマネージメントサブシステムが破壊されないよう確保することである。重要なことは、アクセス制御機能であるＶＬＡＮ、ＶＮＥＴ又は

他のグループ形成をいかに確実に実施するかである。一般に、この活動の一部分は中央で管理され、そして一部分がユーザの判断に委ねられる。従って、グループメンバーシップに対するアクセス制御は、2段階プロセスである。第1段階では、システムアドミニストレータは、グループを形成し、そしてユーザ又はシステムが参加するところのポリシーを確立する。第2段階では、ユーザは、グループに参加することを判断するか、又はシステムをグループに入れることを判断する。次いで、アクセス制御マシンは、グループに関連したポリシーデータを調査し、提案されたメンバーシップ要求が有効であるかどうか決定する。このアクセス制御判断の各段階は、機密保持されねばならない。

他の形式のネットワークマネージメントセキュリティは、マネージメント情報ベース（ＭＩＢ）へのアクセスを制御し、捕獲されたパケットのような重要なネットワークマネージメントデータの保護通信を行い、そしてネットワークマネージメントステーションへのアクセスを与えることである。

第2の重要なネットワークマネージメント問題は、セキュリティポリシーマネージメントである。上記の製品分類の各々は、正しく且つ機密保持されたオペレーションのためにポリシーデータを必要とするセキュリティ特徴を有する。ＮＩＣ、スイッチ、ルータ及びリモートアクセス装置に対するフィルタリングルールが形成され、流布され、変更されそして検討される。中間サイズのネットワークの場合、これらのマネージメント機能は、フィルタリングデータに対して整合された制御がない限り、支持できないことになる。これは、確実且つ頑丈なセキュリティポリシーマネージメントシステムの使用を必要とする。保護通信、アクセス制御及びセキュリティ支援特徴に関連したセキュリティポリシーデータを管理するためには同様の要求が存在する。

フィルタリングパラメータ及び保護通信インフラストラクチャー情報のようなセキュリティポリシーデータを含むネットワークデバイスの数が増加するにつれて、そのセキュリティポリシーデータのコヒレントで且つ整合されたマネージメントを与えることが益々重要となる。本発明によれば、アドミニストレータがセキュリティポリシーステートメントを入力できるようにするツールが設けられ、

このようなステートメントに対応するデータは、そのポリシーが実施されるネットワークに分散されたエージェントへと分布される。

ネットワーク内の種々のデバイスを制御するセキュリティポリシーデータは、種々のやり方で相互作用する。従って、コンフィギュレーションインターフェイスは、ファイアウオール機能の多数の層を正しく管理するのに重要な異なるビューをアドミニストレータに与えるのが好ましい。例えば、ルータのフィルタリングデータは、ソースアドレス、ＴＣＰヘッダ情報、又はソース／行先アドレス対によって表示される。各ビューは、トラフィックが拒絶されるか、許可されるか又は変換されることに関する異なる情報をアドミニストレータに与える。

本発明のコンフィギュレーションドライバーは、所望の振舞いを記述する高レベルのセキュリティポリシーデータを、個々のネットワークデバイスのセキュリティポリシーデータへとマップする。従って、高レベルの記述ポリシーステートメントが低レベルコンフィギュレーションデータのセットへとコンパイルされる。次いで、コンフィギュレーションデータは、例えば、簡単なネットワークマネージメントプロトコル（ＳＮＭＰ）状のプロトコル、テルネット、トリビアルファイル転送プロトコル（ＴＦＴＰ）、又は他のデバイス特有のプロトコルを使用して適当なネットワークデバイスへと分配される。従って、ネットワークトポロジーデータベースは、コンフィギュレーションインターフェイスに与えられるセキュリティポリシーステートメントに基づいてコンフィギュレーションデータをコンパイルしそして分配する目的で重要である。

簡単なネットワークの場合、システムアドミニストレータは、トポロジー情報を手で入力することができる。しかしながら、いかなるサイズのほとんどのネットワークについても、これは実用的なオプションでない。従って、必要なトポロジー情報を維持する従来のネットワークマネージメントツールは、本発明のコンフィギュレーションドライバーに使用するようにトポロジーデータベース情報をコンパイルするのに使用できる。従来のネットワークマネージメントツールによって収集されたトポロジー情報と、本発明のセキュリティポリシー実施戦略との間に必要とされる相互作用のレベルは、実施される多層ファイアウオールの精巧

さに依存する。例えば、ネットワークトポロジーに対する変更は、高レベルセキュリティポリシーデータと、要素デバイスに分配されるセキュリティポリシーデータとの間のマッピングを無効化することがある。精巧な多層ファイアウオールは、トポロジーに変化が生じたときにネットワークマネージメントシステムから通知を受け取り、そしてそれに応じてポリシーデータ及びその要素デバイスを再構成するようにされる。

更に、セキュリティポリシーマネージメントツールは、侵入者がそれを使用してネットワークに侵入できないように保護される。これは、セキュリティポリシーコンフィギュレーションドライバーと、ネットワークに分散されたエージェントとの間の保護通信を適当なアクセス制御手順に基づいて使用することを必要とする。

ネットワークの多数の要素がアクセス制御をサポートする。しかしながら、全ての要素が同じ種類のアクセス制御機構をサポートするのではない。共通のネットワークアクセス制御機能を、ネットワーク内のできるだけ多くのデバイスに与えるのが好ましい。例えば、広範囲に配備された認証、許可及び会計サーバーを、種々様々なネットワークデバイスを管理するように適応させることができる。更に、ネットウェアのようなネットワークオペレーティングシステムは、あるAAAサービスを与える。

更に、ネットワークデバイスは、本発明に基づいてアクセス制御判断を分担することができる。簡単な例では、ラインサーバへのアクセス制御は、スプリットアクセスコンフィギュレーションにおいてそれに関連したパケットサーバに委任することができる。これは、分散型リモートアクセスシステムの一貫した振舞いを確保するだけでなく、その複雑さを低減しそして信頼性を高める。

従来のセキュリティ原理は、保護通信を端から端まで行なわねばならないとしている。しかしながら、動作条件によって時にはこれが最適でないこともある。例えば、資産的装置は、端ー端セキュリティプロトコルをサポートできない。これらのシステム間、又はそれらシステムと非資産的システムとの間の通信のセキュリティを確保するためには、資産的システムの代理として働くルータやスイッチャーのような非侵入の保護機構を必要とする。この解決策は、本来、端ー端ではない。

高いセキュリティを必要とする共通の物理的環境においてある装置を共通配置することができる。このような環境では、境界の外側の装置とその内側の装置との間に端ー端保護を与えることは有益でない。コストを最小限に抑えるために、保護を物理的セキュリティの境界で終わらせ、全ての内部システムの高価なハードウェア及びソフトウェアをサポートする必要性を排除することができる。

セキュリティプロトコルをサポートするには、高価な暗号化ハードウェアを使用することが必要となる。ある場合には、このハードウェアを全てのシステムに経済的に設置することができない。これは、データの最終的な行先より前のどこかで暗号化ハードウェアを実施するシステム又はデバイスでは保護通信経路を終わらせねばならないことを意味する。

これらの状態を受け入れるために、ソースと行先との間の経路の構成セグメントにおいて異なる手段により保護通信を行うことが必要である。幾つかのセグメントは、層3の保護通信を使用し、一方、他のセグメントは、層2の保護を使用する。各セグメントにより与えられる保護を、充分な端ー端セキュリティを確保するように整合するには、これらのセグメントが互いに協働することが必要になる。本発明は、このような協働を管理できるツールを提供する。

図3は、本発明による多層ファイアウオールを実行するのに使用されるプロセスのフローチャートである。上述したように、図3に示すノードは、ネットワーク内の多数のプロトコルレベルで動作する種々様々なネットワークデバイス、最終システム、並びにこれらネットワークデバイス及び最終システムで実行される機能に対応する。

図3に示すように、第1段階は、ネットワークトポロジー及びセキュリティルールを決定する(ステップ300)。この情報は、図1のシステムにおいてコンフィギュレーションインターフェイス及びトポロジーデータ記憶装置によって与えられる。

次いで、ネットワーク内の全ての能動的ノード及び受動的ノードが識別される

(ステップ３０１)。各能動的なノードに対し、能動的なノードを介在せずに能動的なノードに接続された受動的なノードが識別される(ステップ３０２)。これは、能動的ノードのセットを、コンフィギュレーションデータのコンパイルに使用されるべき関連する受動的ノードと共に定義する。例えば、図２を参照すれば、能動的ノードは、ポリシーを実施することのできるノードを含む。受動的ノードは、ポリシーの実施が与えられないか又は信頼されないノードを含む。従って、受動的ノードは、最終システム１４３、中継器１４２、スイッチ１４１、スイッチネットワーク１４０、スイッチ１２４、中継器１２５、及びネットワーク内の他のデバイスを含む。

各セキュリティポリシールールに対し、最終ステーションのソース及び行先セットが識別される(ステップ３０３)。ソース及び行先セットは、各々、単一の最終ステーション又は最終ステーションのグループを含む。次いで、プロセスは、ルールを実施できるかどうか決定する(ステップ３０４)。上述したように、これは、例えば、ソースセットの受動的ノードから行先セットの受動的ノードへ至る経路であって、ルールを実施すべきプロトコル層において動作する能動的ノードを横断しない経路があるかどうか決定することを含む。ソース及び行先セットにおいて受動的ノード間の接続が見つかった場合には、ルールを実施することができない。従って、ルールを実施できない場合には、セキュリティプロセスに通知され(ステップ３０５)、そしてアルゴリズムは、コンパイルされるべきルールがまだあるかどうか決定する(ステップ３０６)。コンパイルされるべきルールがそれ以上残されていない場合には、ステップ３０７で示すように、アルゴリズムは終了となる。更にルールがセキュリティポリシーに存在する場合には、アルゴリズムは、ステップ３０３へループして戻る。

ステップ３０４において、セット内の識別された能動的ノードでルールを実施できることが決定された場合には、次いで、そのルールがソースで実施されるか、行先で実施されるか又はその両方で実施されるよう意図されたかどうか決定される。ルールがソースで実施されるべきであることを指定する場合には、ソースセットのノードと行先セットのノードとの間に介在する能動的ノードが識別され、そしてルールは、ソースノードの１つがその関連セットにあるところの能動的ノードのコンフィギュレーションデータに変換され、そしてこれらノードにおいて確立される(ステップ３１０)。

ルールを行先において実施するか又は行先及びソースの両方において実施すべき場合には、行先セットのノードに関連した各能動的ノードに対し、ルールは、その能動的ノードのコンフィギュレーションデータに変換され、次いで、そのノードにおいて確立される(ステップ３１１)。

ステップ３１０及び３１１の少なくとも１つの後に、アルゴリズムは、変換されるべきルールがもっとあるかどうか決定する(ステップ３１２)。それ以上のルールがない場合には、アルゴリズムは終了となる(ステップ３０７)。変換されるべきルールがもっとある場合には、アルゴリズムは、ステップ３０３へループして戻り、プロセスを続ける。

ソース及び行先セットが識別されると、行先セットのノードに到達するために能動的ノードを横断する必要のない経路が受動的ノード間にあるかどうかを決定するプロセスは、ＷＡＮ１００に接続されたプライベートネットワーク１０２及びスタンドアローン最終システム１０３を考慮することによって理解することができる。これらネットワークセグメントにおけるノードは、ポリシーを実施できないか、又はポリシーを実施する信頼がない。従って、プライベートネットワーク１０２及びスタンドアローンのルータ型最終システム１０３のノードが、特定のルールに対し、ソース及び行先ノードセットに各々存在する場合には、そのルールをこれらノード間で実施することができない。しかしながら、ノード１０３及びプライベートネットワーク１０２の両方が、特定のルールに対してソースノードセットに存在するが、プライベートネットワーク１０１の全てのノードが、特定のルールに対して行先セットに存在する場合には、おそらくルールを実施できることになる。というのは、ソースセットと行先セットとの間を通信するために、全ての通信がルータ１０７、パケットサーバ１０８又はルータ１０９のいずれかを横断しなければならず、これらは全てポリシーを実施できるからである。

図４は、ある環境において多層ファイアウオールを改良することのできるプロ

セスを示す。例えば、図3のステップ303において、プロセスは、ソース及び行先セットのノード間の経路（1つ又は複数）において能動的ノードの「最小カット頂点セット」を識別するように分岐する（ステップ400）。カット頂点セットとは、除去された場合にソースセットと行先セットとを分離する能動的ノードのセットより成る。最小カット頂点セットとは、所与のソース及び行先セットに対して最小数のノードを有するセットである。従って、図2を参照すれば、例えば、ソースセットが最終ステーション113、114、116及び117を含み、そして行先セットがスタンドアローンのルータ型最終システム103である場合に、能動的ノードの最小カット頂点セットは、リモートアクセスルータ112より成る。

リモートアクセスルータ112を通る各経路には、ソースセットに関連した能動的ノード（112及び115）及び行先セットに関連した能動的ノード（104及び106）に見られるものより少数の能動的ノードしかないので、ある場合には、最小カット頂点セットの能動的ノードでのセキュリティポリシーの実施を、セキュリティポリシーをソース及び行先セットの全ての能動的ノードへ分配して実施するものよりも効率的に行うことができる。従って、アルゴリズムは、次いで、最小カット頂点セットの能動的ノードにおいてルールを効率的に実施できるかどうか決定する（ステップ401）。もしそうでなければ、アルゴリズムは、ステップ402で示されたように、図3のステップ304へ復帰する。最小カット頂点セットの能動的ノードにおいてルールを実施できる場合には、ルールが、カット頂点セットにおける能動的ノードのコンフィギュレーションデータに変換され、そしてこのようなノードにおいて確立される（ステップ403）。ステップ403の後に、プロセスは、図3のアルゴリズムのステップ304へ復帰する。

図5は、ネットワークを通して分散されたセキュリティポリシーエージェントにおいてコンフィギュレーションデータを確立するためのプロセスを示す。

より詳細には、ノードにルールを確立するプロセスは、コンフィギュレーションデータをノードに転送し、それを永続的記憶装置に記憶し、そして新たなルールを実行できるようにデータが更新されたことをノードに確認させることを含む

。しかしながら、ネットワークに分散された全てのセキュリティエージェントが、ディスクドライブや不揮発性フラッシュメモリデバイスのような永続的記憶装置に直接接続されるのではない。例えば、中継器133は、永続的記憶能力をもたないことが考えられる。しかしながら、スイッチ123、又は更に好ましくは、ポリシーマネージメントステーションの一部分を形成する最終ステーション126は、ディスクドライブ又は他の永続的記憶能力を有する。この状態において、コンフィギュレーションデータをスイッチ123、最終ステーション126又はネットワーク内の別のサーバに与え、そしてコンフィギュレーションデータが更新されたことを中継器133に通知することができる。中継器133に関連したマネージメントエージェントは、次いで、再ブートの際に、又はコンフィギュレーションデータを更新する必要のある他のプロセスの間に、スイッチ123又は

最終ステーション126からコンフィギュレーションデータを検索する。

従って、ノードにルールを確立するプロセスが図5に示され、ステップ500で始まる。このプロセスは、先ず、コンフィギュレーションデータの対象ノードが永続的なコンフィギュレーション記憶装置を含むかどうか決定する（ステップ501）。もしそうであれば、コンフィギュレーションデータがそのノードの永続的な記憶装置へ送られる（ステップ502）。ノードが永続的な記憶装置を含まない場合には、コンフィギュレーションデータの対象ノードによってアクセスできるノードの永続的な記憶装置にコンフィギュレーションデータが送られる（ステップ503）。次いで、コンフィギュレーションデータの対象であるノードに変化を示す信号が送られる（ステップ504）。変化が生じたという信号を受信した後に、ノードは、更新されたコンフィギュレーションデータを検索する（ステップ505）。ステップ502又はステップ505のいずれかによってコンフィギュレーションデータがノードに送られた後に、ノードは、それが受け取ったコンフィギュレーションデータに基づいて新たなルールを実行する（ステップ506）。

従って、セキュリティポリシーマネージメントコンフィギュレーションドライ

バーは、これらルールのコンフィギュレーションデータをノードに通信することによりノードにルールを確立する。例えば、ノードが永続的な記憶装置を有する場合には、セキュリティポリシーマネージメントコンフィギュレーションドライバーは、テルネット又はトリビアル・ファイル搬送プロトコル（ＴＦＴＰ）のような標準的なプロトコルを使用してルールをノードへ直接通信するか、又は多層ファイアウオールの一部分としてこの目的のために特に指定されたプロトコルを使用する。ノードが永続的な記憶装置をもたない場合には、セキュリティポリシーマネージメントコンフィギュレーションドライバーは、ノードによってアクセスできる永続的な記憶装置にルールを通信し、次いで、例えば、ＳＮＭＰ又は別のプロトコルを用いてノードに信号を送り、セキュリティポリシールールが更新されたことをノードに通知する。次いで、ノードは、新たなセキュリティポリシールールを永続的な記憶装置から検索することができる。更に、別のシステムにおけるセキュリティポリシーマネージメントコンフィギュレーションドライバーが分散型データベース解決策を用いてノードポリシーを更新する。例えば、セキュリティポリシーマネージメントコンフィギュレーションドライバーは、ノードがキャッシュコピーを有するところのファイル又はデータベースエントリーにデータを書き込むことができる。この分散型データベースキャッシュコヒレンシーアルゴリズムは、次いで、そのキャッシュコピーがもはや有効でないことをノードに通知し、マスターコピーを再読み取りするよう動機付ける。

各能動的ノードにおいてルールを実施すべきかどうか決定するための上記アルゴリズムは、本発明の多層ファイアウオールシステムの能力を例示するものに過ぎない。他のアルゴリズムも考えられる。例えば、セキュリティポリシーステートメントは、特定のセキュリティポリシールールにおいて、異なる能動的ノードで実施される部分に分解することができる。これは、ソースセットのノードと行先セットのノードとの間の経路を分析し、この経路における各能動的ノードにサポートされる意味を決定し、そしてこのセットの能動的ノードにおいてポリシールールの種々のセグメント又はポリシールールの冗長バージョンを実施することを必要とする。これらの能動的ノードにおいてセキュリティポリシールールを順

次に適用すると、ソース、行先、又はカット頂点セットの能動的ノードにおいて実施することのできないポリシーを実施できるので、分散形態でルールを実施するこの解決策は、より効率的なファイアウオールを与えることができる。更に、ノードの順次経路に沿ってポリシールールの実施を分解することにより、ソース、行先又はカット頂点セットの能動的ノードにおける実施では考えられない効率を与えることができる。

図６及び７（図２と同様）を参照して説明する２つの例は、多層ファイアウオールが実際にいかに作用するかを示す。図６及び７において、ホストグループ１（６００）は、中継器（６０４及び６０５）及びスイッチ（６０６及び６０７）を経て２つのサイトルータ６０８の一方に接続された多数の最終システム６０１、６０２、６０３…より成る。ホストグループ２（６１０）は、中継器６１３及びスイッチ６１４を経て他のサイトルータ６１５に接続された２つの最終システム（６１１及び６１２）より成る。２つのサイトルータは、スイッチ６２０を経て相互接続される。

両方の例において、多層ファイアウオールは、１つのポリシールールで構成される。

ソース	行先	アクティビティ	ポリシーステートメント	実施場所
ホストグループ２	ホストグループ１	ＦＴＰ	許可	両方

このルールは、多層ファイアウオールポリシーマネージメントステーション６２５においてセキュリティアドミニストレータによって入力される。

第１の例（図６）においては、２つのスイッチ６０６及び６０７は、中継器６０４及び６０５を経てホストグループ１（６００）に接続され、ファイアウオールルールの実施を行うことができ、そしてスイッチ６１４及び中継器６１３によりホストグループ２（６１０）に接続されたサイトルータ６１５も、ファイアウオールルールの実施を行うことができる。

多層ファイアウオールポリシーマネージメントステーション６２５は、多層フ

ァイアウオールポリシールールを２つのノード特有のポリシールールに分解し、その一方は、サイトルータ６１５に対するものであり、そしてその他方は、２つのスイッチ６０６及び６０７に対するものである(両スイッチは、同じデバイス特有のポリシールールを受け入れると仮定する)。「実施場所」の項は、「両方」を指定しているので、多層ファイアウオールポリシーマネージメントステーション６２５は、ノード特有のポリシールールを、ＴＦＴＰのようなプロトコルを使用するサイトルータ６１５と、ＴＦＴＰのようなプロトコル又は下位層ＳＮＭＰを使用する２つのスイッチ６０６及び６０７との両方にダウンロードする。「実施場所」の項が「ソース」を指定する場合には、多層ファイアウオールポリシーマネージメントステーション６２５は、サイトルータ６１５に対するポリシールールのみをダウンロードする。「実施場所」の項が「行先」を指定する場合には、多層ファイアウオールポリシーマネージメントステーション６２５は、スイッチ６０６及び６０７に対するポリシールールのみをダウンロードする。

第２の例（図７）は、第１の例と同じネットワークトポロジーを有する。しかしながら、ポリシーの実施は、第１の例とは異なるやり方で行なわれる。特に、中継器６０４及び６０５を経てホストグループ１（６００）の最終システムに接続されたスイッチと、これらの最終システムにおけるＮＩＣとの両方は、ノード特有のポリシールールを実施することができる。加えて、中継器６１３を経てホストグループ２（６１０）に接続されたスイッチ６１４は、ノード特有のポリシールールを実施できるが、サイトルータ６１５は、実施できない。

多層ファイアウオールポリシーマネージメントステーション６２５は、多層ファイアウオールのポリシールールを２つのノード特有のポリシールールに分解し、その一方は、中継器を経てホストグループ２（６１０）に接続されたスイッチ６１４に対するものであり、そしてその他方は、ホストグループ１（６００）に接続された２つのスイッチ６０６及び６０７に対するものである(この場合も、これらスイッチの両方が、同じデバイス特有のポリシールールを受け入れると仮定する)。「実施場所」の項は、「両方」を指定しているので、多層ファイアウオールポリシーマネージメントステーション６２５は、ノード特有のポリシールー

ルを、ホストグループ２（６１０）のスイッチ６１４と、ホストグループ１（６００）の２つのスイッチ６０６及び６０７との両方にダウンロードする。「実施場所」の項が「ソース」を指定する場合には、多層ファイアウオールポリシーマネージメントステーション６２５は、適当なポリシールールをホストグループ２（６１０）のスイッチ６１４のみにダウンロードする。「実施場所」の項が「行先」を指定する場合には、多層ファイアウオールポリシーマネージメントステーション６２５は、適当なポリシールールをホストグループ１（６００）のスイッチ６０６及び６０７のみにダウンロードする。

この例は、ＮＩＣが多層ファイアウオールに参加する１つの方法も示している。ホストグループ１（６００）に関連した各スイッチ６０６及び６０７は、そのノード特有のポリシールールを受け取ると、それが接続されたホストグループ１（６００）の各最終システム６０１、６０２及び６０３へポリシールール情報を放送する。例えば、ホストグループ１（６００）のスイッチ６０６及び６０７に対するノード特有のポリシールールは、次のようになる。

ソース	行先	アクティビティ	ポリシーステートメント
ホスト611	ホスト601	ＦＴＰ	許可
ホスト612	ホスト601	ＦＴＰ	許可
ホスト611	ホスト602	ＦＴＰ	許可
ホスト612	ホスト602	ＦＴＰ	許可
*	*	*	*
*	*	*	*
*	*	*	*

このテーブルにおいて、ホストグループ２（６１０）の各最終システム６１１及び６１２は、行先であるホストグループ１（６００）の各ホストに対するソースとして特にリストされている。実際の場合には、ホストグループ２（６１０）及びホストグループ１（６００）の最終システムに関連したサブネットアドレスをリストすることによりこれらルールをより効率的に表すことができる。

最終システム６０１のＮＩＣのような各ＮＩＣは、これらのルールを受け取る

と、その最終システム（例えば、６０１）が行先ではないところのノード特有のポリシールールを全て破棄する。次いで、残りのルールを使用して、最終システム（例えば、６０１）に到着するパケットをフィルタする。この例では、ノード特有のポリシールールを実施するＮＩＣを伴う最終システム６０１、６０２及び６０３は、ホストグループ２（６１０）における最終システム６１１及び６１２からのＦＴＰ要求以外のトラフィックを受け取ることができない。

ホストグループ１（６００）のスイッチ６０６及び６０７は、これらのルールを使用するが、ホストグループ１（６００）の最終システム６０１、６０２及び６０３から到来するトラフィックに対してのみである。特に、それらは、ホストグループ２（６１０）の最終システム６１１及び６１２を行先とするＦＴＰ応答ではない全てのパケットをドロップする。これらのスイッチ６０６及び６０７は、それらが中継器６０４及び６０５を経て接続されない最終システムの行先アドレスを特定するノード特有のルールを破棄する。

この例において示される効果は、ＮＩＣがインバウンドトラフィックに対して多層ファイアウオールポリシールールを実施する役割を果たし、一方、スイッチがアウトバウンドトラフィックに対してそれを実施する役割を果たすことである。この実施に対する役割を分割することにより、ホストグループ１（６００）のスイッチ６０６及び６０７からある処理の負荷を取り去る。敵対するトラフィック

に対して最終システムを保護するようにＮＩＣに依存することによりこれが行なわれる。

両方の例において、多層ファイアウオールマネージメントステーション６２５は、デバイス特有のポリシールールをデバイスへ直接通信する。この解決策は、説明を簡略化するが、多層ファイアウオールマネージメントプロトコルに複雑さをもたらす。他の実施戦略も考えられ、望ましいものがある。例えば、ノード特有のポリシールールをデバイスに直接分配するのではなく、多層ファイアウオールマネージメントステーション６２５は、それらを永続的記憶装置に記憶し、そして新たなポリシーを検索するように各デバイスに通知することができる。第２

の例では、ホストグループ１（６００）のスイッチ６０６及び６０７は、最終システム６０１、６０２及び６０３のＮＩＣにノード特有のポリシーを直接放送するのではなく、永続的な記憶装置から新たなポリシーを検索すべきであることを通知するメッセージをそれらに放送してもよい。

本発明の多層ファイアウオール機能は、１つの実施形態では、オブジェクトベースのマネージメントシステムとして実施され、そして他の実施形態では、分散型多層ファイアウオールの構成を与える目的で他のプログラミング技術で実施される。

本発明は、種々様々なネットワークデバイス及び最終システムより成るネットワークにおいて整合された多層型の浸透したファイアウオールを形成するフレームワークを提供する。このシステムは、セキュリティポリシールールを高レベルで指定するコンフィギュレーションインターフェイスをベースとする管理し易い前端を与える。これらのルールは、次いで、ルールによって作用を受けるネットワーク内のノードに対する実際のコンフィギュレーションデータに分解される。このコンフィギュレーションデータは、次いで、ルールを実施するためにネットワークのノードにおいて確立される。ネットワークのトポロジー及びネットワークのノードで実行されるセキュリティ機能の形式に関する情報を使用して、このプロセスをルールごとに実行することにより、整合された浸透した多層ファイアウオールシステムが提供される。本発明によれば、ファイアウオールの種々の要素の役割分担が、好ましくは、グラフィックユーザインターフェイス及び高レベ

ルスクリプトのような使い易い特徴を実施する１つ以上のインテリジェントマネージメントシステムに集合される。

本発明の多層ファイアウオールは、無類の融通性をもつネットワークシステムのセキュリティインフラストラクチャーを提供する。更に、種々様々なネットワークにおける多数のデバイスの複雑な管理を可能にするコヒレントな前端が提供される。

本発明の好ましい実施形態の以上の説明は、本発明を単に例示するものに過ぎない。本発明は、これに限定されるものではなく、請求の範囲に記載した本発明

の範囲内で多数の種々の変更がなされ得ることが当業者に明らかであろう。

【図1】

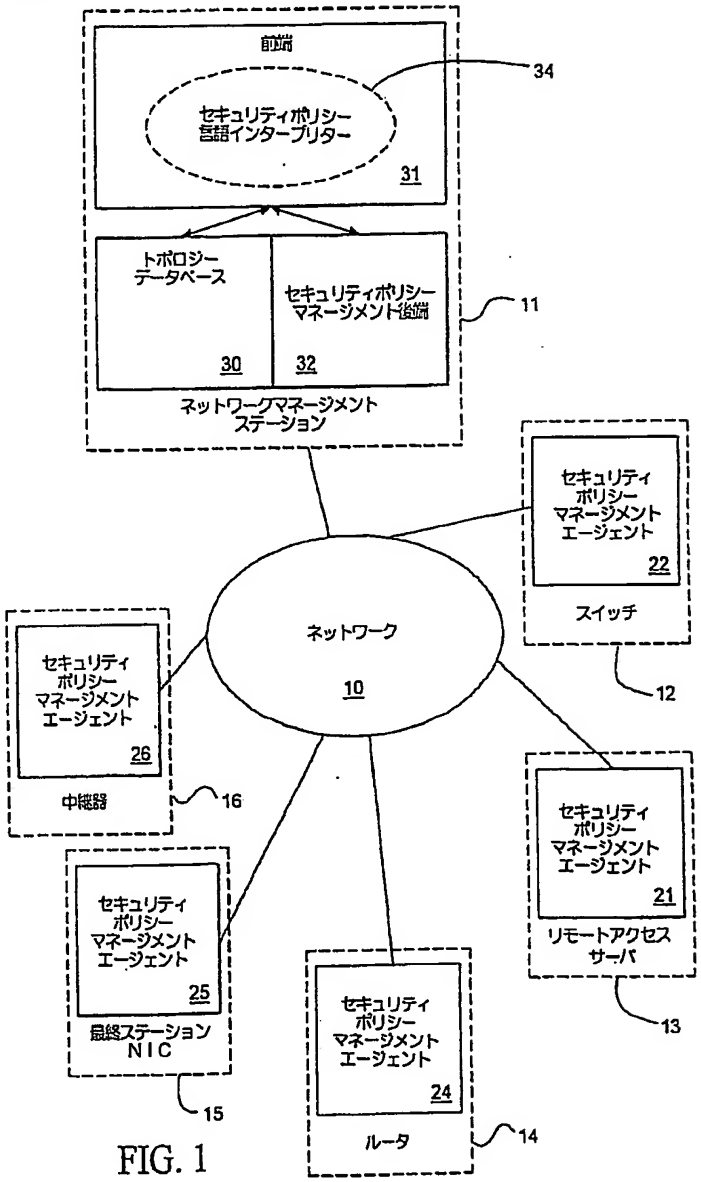

FIG. 1

【図2】

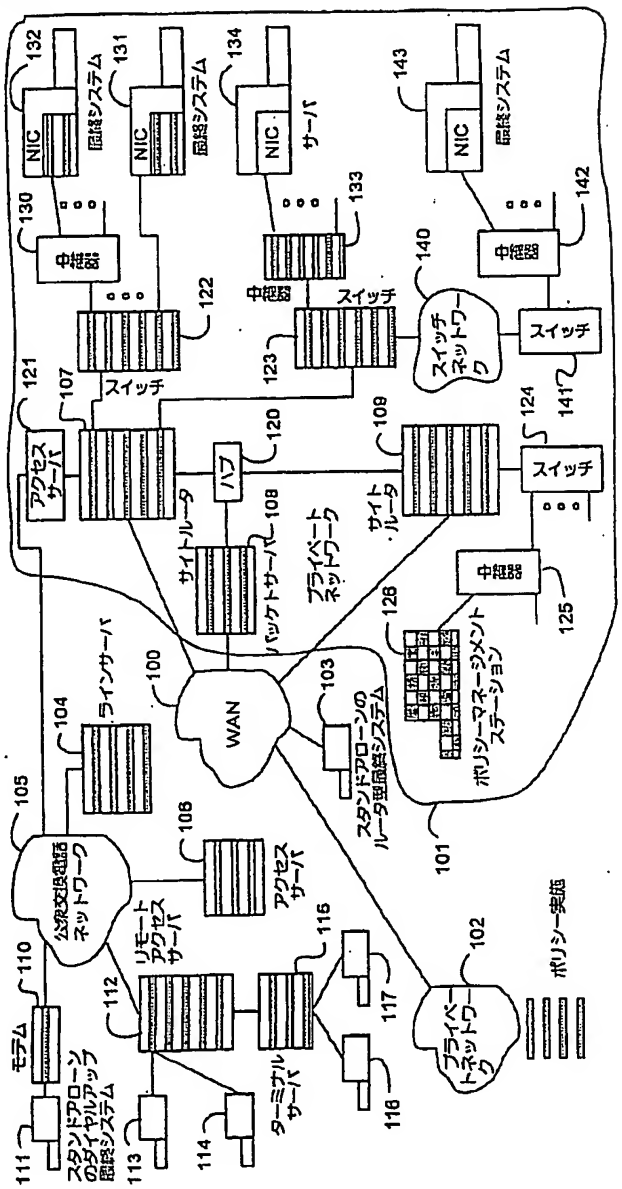

FIG. 2

【図3】

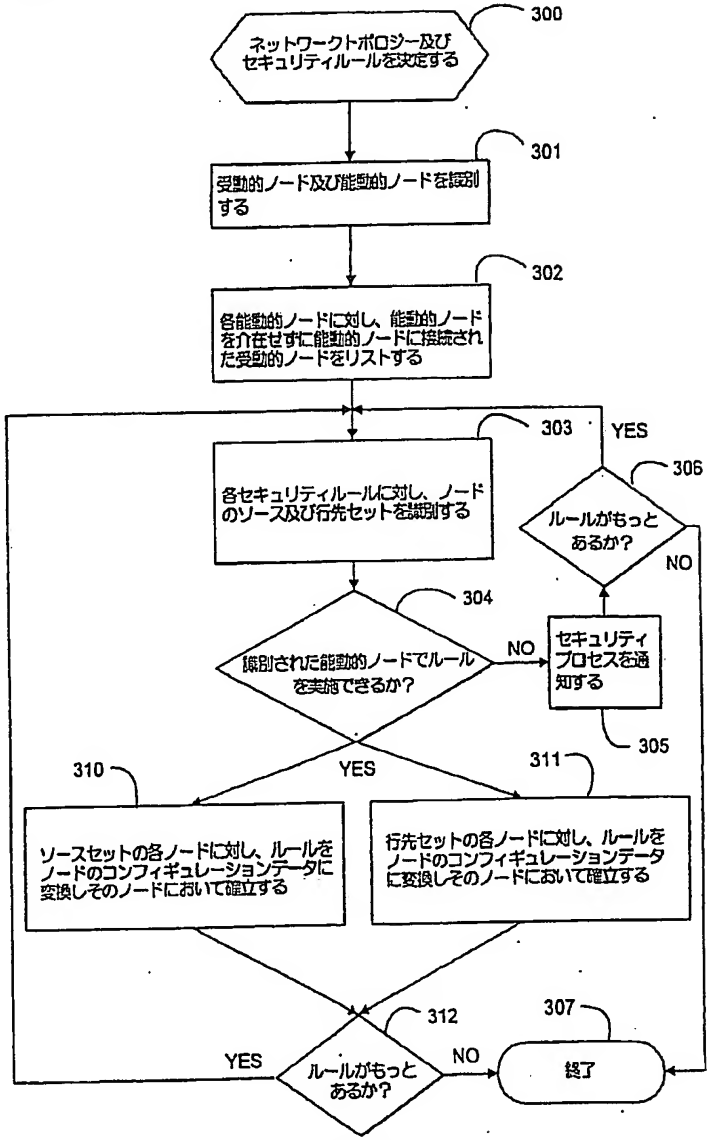

FIG. 3

【図4】

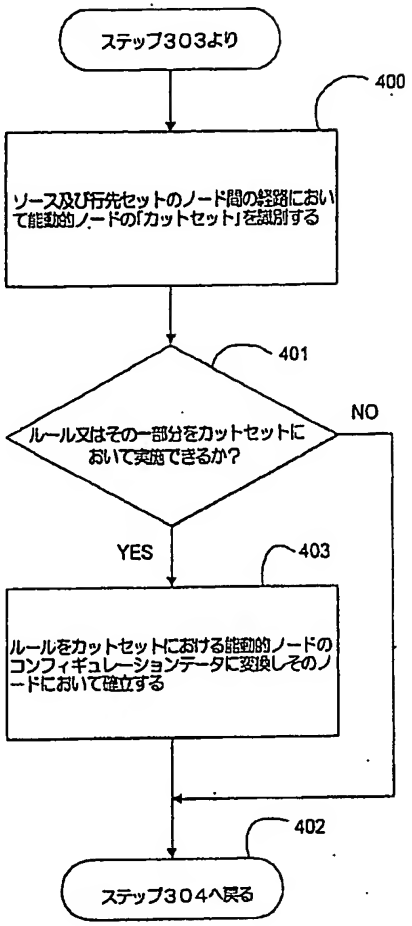

FIG. 4

【図5】

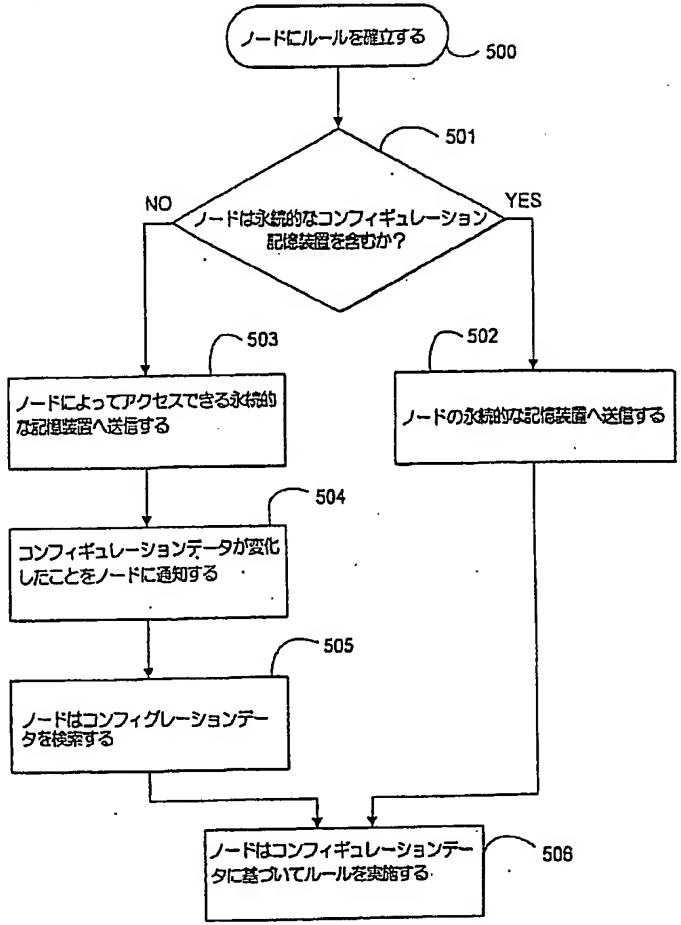

FIG. 5

【図６】

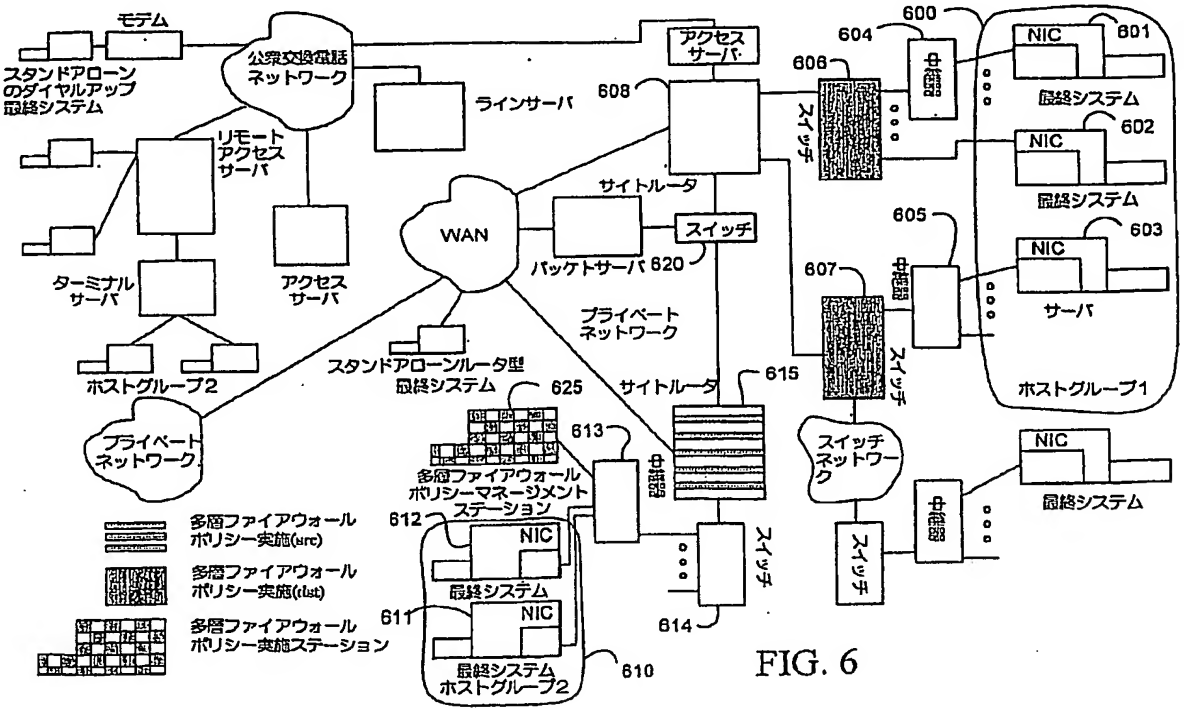

FIG. 6

【図７】

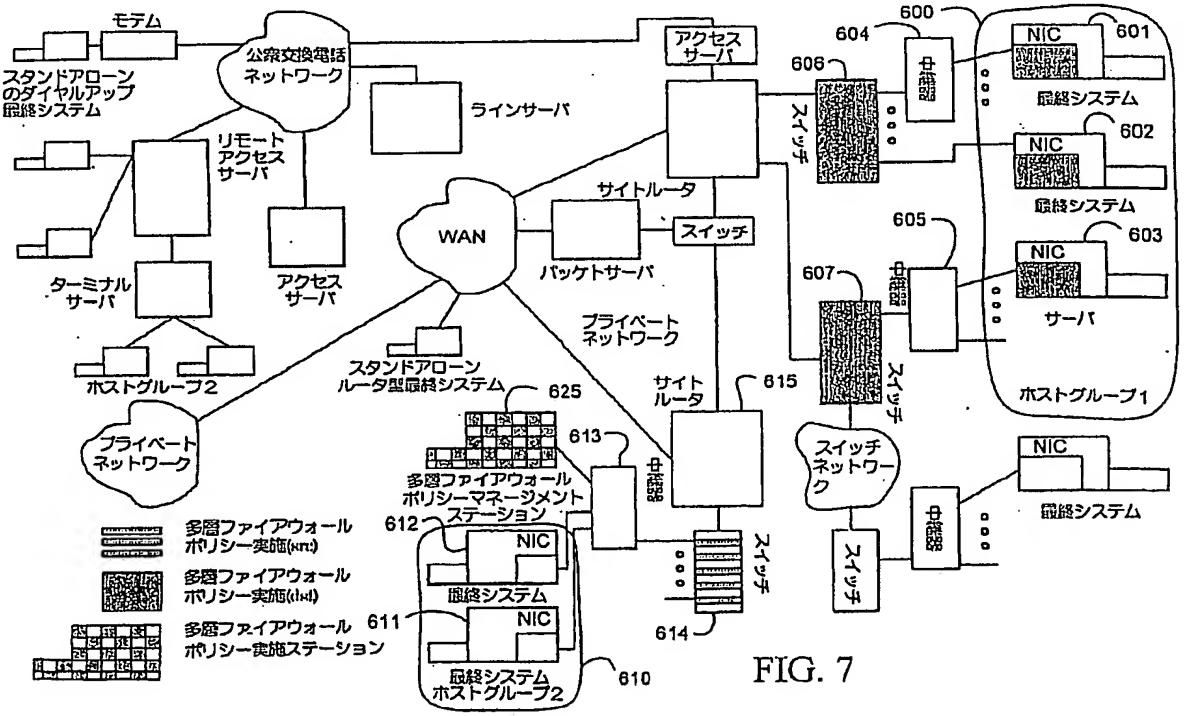

FIG. 7

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No. PCT/US98/10817

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G06F 11/00
US CL :395/187.01
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 395/187.01, 188.01, 186, 200.59, 200.53, 683; 380/23, 25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
APS, INTERNET

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CHECK POINT SOFTWARE TECHNOLOGIES LTD. "Check Point Software Unveils Open Security Platform Strategy". http://www.checkpoint.com. 18 November 1996. See entire document.	1-15, 17, 21-22, 24-25, 43, 45-49 and 55-63
Y	SIMON et al. "Adage: An Architecture for Isrtibuted Authorization". OSF Research Institute. 2 December 1996. pp. 13-17.	1-15, 17, 21-22, 24-25, 43, 45-49 and 55-63
Y, P	US 5,740,375 A (DUNNE et al) 14 April 1998, col. 1, lines 22-34; col. 3, lines 12-32.	2-5, 9-14 and 55-58
A	US 4,881,263 A (HERBISON et al) 14 November 1989, col. 19, lines 8-42.	1-71

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 AUGUST 1998	29 SEP 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer ROBERT BEAUSOLIEL Telephone No. (703) 305-9711

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No. PCT/US98/10817

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,577,209 A (BOYLE et al) 19 November 1996, see entire document.	1-71
A	US 5,606,668 A (SHWED) 25 February 1997, see entire document.	1-71
A	BLAZE et al. "Decentralized Trust Management". IEEE Conference on Security and Privacy. May 1996. See entire document.	1-71
A	CHECK POINT SOFTWARE TECHNOLOGIES LTD. "Check Point Software Brings 'Write Once, Manage Everything' Functionality to Enterprise Security Management". http://www.checkpoint.com. 22 October 1997. See entire document.	1-71
A	CHECK POINT SOFTWARE TECHNOLOGIES LTD. "Open Security Manager Data Sheet". http://www.checkpoint.com. 1998. See entire document.	1-71

Form PCT/ISA/210 (continuation of second sheet)(July 1992)*